UNIVERSIDAD TECNOLÓGICA ISRAEL

ESCUELA DE POSGRADOS "ESPOG"

MAESTRÍA EN SEGURIDAD INFORMÁTICA

Resolución: **RPC-SO-02-No.053-2021**

PROYECTO DE TITULACIÓN EN OPCIÓN AL GRADO DE MAGÍSTER

Título del proyecto:
Análisis de Vulnerabilidades basado en Técnicas de Inteligencia Artificial para la Seguridad Informática en Redes de Área Local.
Línea de Investigación:
Ciencias de la ingeniería aplicadas a la producción, sociedad y desarrollo Sustentable.
Campo amplio de conocimiento:
Tecnologías de la Información y Comunicación (TIC)
Autor:
Byron David Villacís Calles
Tutor:
PhD. Maryory Urdaneta Herrera MSc. Renato Mauricio Toasa Guachi

Quito – Ecuador

2024

APROBACIÓN DEL TUTOR

Yo, PhD. Maryory Urdaneta Herrera con C.I: 1759316126 en mi calidad de Tutor del proyecto de investigación titulado: Análisis de Vulnerabilidades basado en Técnicas de Inteligencia Artificial para la Seguridad Informática en Redes de Área Local.

Elaborado por: Byron David Villacís Calles, de C.I: 1600443004, estudiante de la Maestría: Seguridad Informática, de la **UNIVERSIDAD TECNOLÓGICA ISRAEL**, como parte de los requisitos sustanciales con fines de obtener el Título de Magister, me permito declarar que luego de haber orientado, analizado y revisado el trabajo de titulación, lo apruebo en todas sus partes.

Quito D.M., marzo 2024

Firmado electrónicamente por:
MARYORY URDANETA HERRERA

Firma

APROBACIÓN DEL TUTOR

Yo, MCs. Renato Mauricio Toasa Guachi con C.I: 1804724167 en mi calidad de Tutor del proyecto de investigación titulado: Análisis de Vulnerabilidades basado en Técnicas de Inteligencia Artificial para la Seguridad Informática en Redes de Área Local.

Elaborado por: Byron David Villacís Calles, de C.I: 1600443004, estudiante de la Maestría: Seguridad Informática, de la **UNIVERSIDAD TECNOLÓGICA ISRAEL**, como parte de los requisitos sustanciales con fines de obtener el Título de Magister, me permito declarar que luego de haber orientado, analizado y revisado el trabajo de titulación, lo apruebo en todas sus partes.

Quito D.M., marzo 2024

Firmado electrónicamente por:
RENATO MAURICIO
TOASA GUACHI

Firma

DECLARACIÓN DE AUTORIZACIÓN POR PARTE DEL ESTUDIANTE

Yo, Byron David Villacís Calles, de C.I: 1600443004, autor del proyecto de titulación denominado: Análisis de Vulnerabilidades basado en Técnicas de Inteligencia Artificial para la Seguridad Informática en Redes de Área Local. Previo a obtener el título de Magister en Seguridad Informática.

Declaro tener el pleno conocimiento de la obligación que tienen las instituciones de educación superior, de conformidad con el Artículo 144 de la Ley Orgánica de Educación Superior, de entregar el respectivo trabajo de titulación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.

Manifiesto mi voluntad de ceder a la Universidad Tecnológica Israel los derechos patrimoniales consagrados en la Ley de Propiedad Intelectual del Ecuador, artículos 4, 5 y 6, en calidad de autor@ del trabajo de titulación, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente. En concordancia suscribo este documento en el momento que hago entrega del trabajo final en formato impreso y digital como parte del acervo bibliográfico de la Universidad Tecnológica Israel.

Autorizo a la SENESCYT a tener una copia del referido trabajo de titulación, con el propósito de generar un repositorio que democratice la información, respetando las políticas de prosperidad intelectual vigentes.

Quito D.M., marzo de 2024

Firmado electrónicamente por:
BYRON DAVID
VILLACIS CALLES

Firma

Orcid: 0000-0003-1343-2147

Tabla de contenidos

Índice de tablas

Índice de figuras

INFORMACIÓN GENERAL

Contextualización del tema

El análisis y detección de vulnerabilidades hace referencia a la identificación de las debilidades de un sistema informático o su entorno, las cuales pueden ser aprovechas por atacantes, comprometiendo su integridad, confidencialidad y la disponibilidad de la red (Suárez Panchana, 2022). Solo en el primer trimestre de 2022 se reportaron más de 8000 nuevas vulnerabilidades, un 25% más alto en relación a 2021; se encontró que 1 de cada 10 tenían una consideración de alto riesgo; por otra parte, las empresas de tamaño mediano y pequeñas son las que tienen un alto riesgo (NVD, 2023).

Ante el incremento de la complejidad de las diferentes infraestructuras y aplicaciones que involucran a las tecnologías de la información (TI) y el crecimiento de las amenazas cibernéticas, la inteligencia artificial (IA) y sus aplicaciones en todo ambiente, han llegado a ser un recurso para identificar y contrarrestar vulnerabilidades en la protección de datos. En este sentido, las diferentes técnicas de IA se han destacado en procesar automáticamente las vulnerabilidad detectadas, reduciendo los tiempo de trabajo tanto para su identificación y respuesta, en relación a profesionales entrenados para en este tipo de trabajos (Rasthofer y Arzt, 2014).

El concepto de "Inteligencia Artificial" fue acuñado en 1956, marcando el inicio de su evolución hacia aplicaciones prácticas en una amplia gama de campos (Alom et al., 2018). La contribución del aprendizaje automático a la ciberseguridad comenzó en la década de 1990 con el desarrollo de Sistemas de Detección de: Anomalías (ADS) y de intrusiones (IDS), aunque su avance inicial se limitó por restricciones computacionales (Qiu, 2016). Actualmente, la IA y sus herramientas demuestran ser un elemento clave dentro la ciberseguridad, dentro del ámbito corporativo, siendo capaz de emular la inteligencia y comportamientos humanos para automatizar y detectar brechas de seguridad en redes en cuestión de segundos (Zeadally et al., 2020).

La pandemia de COVID-19 impulsó la transformación digital, incrementando la dependencia de nuevas tecnologías, tales como los con las herramientas de IA, el aprendizaje automático (ML) y los big data, lo que a su vez también ha elevado los riesgos de delitos cibernéticos, amenazando a individuos y organizaciones (Zhang et al., 2022). Se proyectan que los delitos cibernéticos podrían costar hasta 10.5 billones de dólares para 2025, presentando desafíos significativos de riesgo operativo y continuidad para las empresas. Por lo que, día a día se destaca la importancia de explorar el uso de la IA en la ciberseguridad para que las organizaciones puedan aprovechar sus capacidades en beneficio propio (Eian et al., 2020).

La IA ha despegado en su utilización a todo tipo de nivel, sea personal o corporativo, hasta el punto de que ahora es posible utilizar procesamiento de lenguaje natural (PLN), pruebas automatizadas y análisis de código de manera significativa. Las grandes cantidades de nuevos dispositivos, herramientas y aplicaciones que se están desplegando hoy en día no solo aumenta los riesgos de vulnerabilidades en un sistema en red, sino que también proporciona una amplia colección de datos de entrenamiento para las IA (Kommrush, 2018)

Es importante, tomar en cuenta que la IA al ser software, sus modelos son susceptibles a las mismas vulnerabilidades que los programas tradicionales. Sin embargo, el uso de la IA en la seguridad de redes es un arma de doble filo; mientras que los proveedores de seguridad utilizan herramientas basadas en IA para manejar automáticamente incidentes de seguridad, los actores de amenazas también pueden usar esta tecnología para desarrollar programas maliciosos inteligentes (NSFOCUS, 2023).

En este sentido, es necesario abordar los riesgos de la IA como una extensión de los riesgos digitales ya conocidos, utilizando frameworks y estrategias de gestión de riesgos ya existentes. Así como, incluir explícitamente la IA en las actividades como la divulgación y gestión de vulnerabilidades, para garantizar una protección integral de toda la red (Dempsey, 2021).

Por lo expuesto, la IA se perfila como una herramienta clave en la detección y mitigación de vulnerabilidades en redes de área local. A pesar de sus potenciales ventajas, la implementación de la IA enfrenta desafíos, como la susceptibilidad a vulnerabilidades y la integración con estrategias de gestión de riesgos existentes, haciendo del análisis de vulnerabilidades basado en IA un campo investigación continua para fortalecer la seguridad informática la dinámica cambiante de las amenazas digitales.

Problema de investigación

Las redes de área local (LAN) constituyen elementos fundamentales en la arquitectura tecnológica de una amplia gama de entidades corporativas, proporcionando infraestructura esencial para la facilitación del intercambio de comunicaciones y el acceso a recursos distribuidos. Sin embargo, dichas redes son propensas a un extenso número de vulnerabilidades técnicas que pueden ser explotadas por agentes maliciosos con el objetivo de comprometer los pilares de seguridad de datos: integridad, confidencialidad y disponibilidad. Los ataques que llegan a explotar estas falencias no solo tienen el potencial de desestabilizar las operaciones de la organización, sino que también puede conllevar consecuencias financieras, deterioro de la imagen corporativa, ya que, se pierde la confianza

ante la falta de privacidad y protección de información sensible de los clientes y en general de toda la organización en su conjunto.

La detección de vulnerabilidades en tales entornos se ve obstaculizada por diversas limitaciones, incluidos los recursos de infraestructura y la capacidad de procesamiento de datos. Además, el tiempo de respuesta para la detección y solución de vulnerabilidades por parte del personal de TI a menudo se ve afectado por la carga de trabajo y la complejidad de los nuevos ataques. Este retraso en la respuesta puede dejar a las empresas vulnerables a ataques durante largos períodos de tiempo, con mayores niveles de riesgos y consecuencias de posibles brechas de seguridad.

Por lo mencionado, el uso de la inteligencia artificial (IA) como un elemento para enfrentar dichos obstáculos. Mediante la automatización y el análisis avanzado de datos, la IA posee la capacidad de fortalecer la identificación y la atenuación de vulnerabilidades, disminuyendo la necesidad de acciones manuales y agilizando el proceso de reacción ante incidentes de seguridad. Por lo que, la investigación y propuesta tiene como finalidad dar respuesta a la siguiente interrogante ¿Cuáles son las técnicas y herramientas de inteligencia artificial más efectivas actualmente, tanto para la detección y el análisis de vulnerabilidades en redes LAN?

Objetivo general

Realizar un análisis de las vulnerabilidades utilizando herramientas de inteligencia artificial para la seguridad informática en redes de área local, para determinar los beneficios de emplear esta tecnología.

Objetivos específicos

1. Contextualizar fundamentos teóricos, de metodologías y herramientas de inteligencia artificial aplicadas en la seguridad informática en redes de área local para proteger la información.
2. Establecer la metodología a aplicar para el apoyo en la resolución de la problemática mediante métodos investigativos.
3. Realizar un plan de recomendaciones de forma práctica sobre el análisis de vulnerabilidades basado en técnicas de inteligencia artificial.
4. Valorar el impacto sobre el análisis de la interacción de la Inteligencia Artificial con respecto a la seguridad informática.

Vinculación con la sociedad y beneficiarios directos

La presente investigación sobre el análisis de vulnerabilidades utilizando técnicas de inteligencia artificial (IA) en redes de área local tiene el potencial de beneficiar a diferentes

actores, con un impacto significativo en varios sectores. En el ámbito empresarial, las empresas de todos los tamaños podrán fortalecer sus sistemas de seguridad informática, protegiendo sus activos digitales y datos críticos contra las crecientes amenazas hacia sus redes. Esto no solo mejorará su respuesta y continuidad del negocio, sino que también contribuirá a la confianza de los usuarios y otros actores clave de las organizaciones, que ayuden al aseguramiento de la integridad y confidencialidad de la información.

El estudio también fomentará el desarrollo de nuevos conocimientos relacionados con la seguridad en redes y la IA, inspirando nuevas líneas de investigación. Las instituciones educativas podrán integrar estos hallazgos en sus currículos, preparando a la próxima a nuevos profesionales de TI con habilidades actualizadas y relevantes para enfrentar los desafíos de seguridad en la era digital. Por otra parte, la investigación propone una propuesta de recomendaciones que serán elementos base para desarrollo de políticas públicas y estrategias de seguridad nacional, ayudando a las entidades gubernamentales a proteger la infraestructura crítica y los datos sensibles de los ciudadanos.

En última instancia, el personal de TI y los profesionales de la seguridad se beneficiarán directamente de las herramientas y metodologías desarrolladas, ya que facilitarán la identificación y la mitigación de vulnerabilidades con mayor eficiencia. Al reducir la carga de trabajo manual y acelerar la respuesta a las amenazas, estos profesionales podrán centrarse en estrategias de seguridad más complejas y en la innovación. En resumen, esta investigación promete aportar valor tangible a la sociedad, mejorando la seguridad y protección de los datos contra ciberataques en la redes de área local, con el uso de las nuevas herramientas de IA que al día de hoy están disponibles.

CAPÍTULO I: DESCRIPCIÓN DEL PROYECTO

1.1. Contextualización general del estado del arte

Una red de área local (LAN) permite la conexión y compartición de recursos entre dispositivos en una zona geográfica limitada, facilitando la comunicación eficiente dentro de organizaciones o espacios definidos. Entre los tipos de LAN, se encuentran las redes FDDI, que utilizan fibra óptica y siguen el estándar ANSI para el protocolo Token Ring de control de acceso al medio. Las redes Ethernet, por otro lado, apoyan la topología de LAN basada en los estándares de Ethernet Versión 2 e IEEE 802.3. Además, las redes Token Ring distribuyen datos en una secuencia predeterminada, mientras que las redes inalámbricas ofrecen mayor movilidad a los empleados, siendo ideales para conectar la oficina con sitios externos a través de sistemas de transacciones portátiles (IBM, 2021)

La protección de los datos ha llegado a convertirse en un elemento crítico para todas las entidades, debido a que las redes de comunicaciones enfrentan un riesgo creciente de ser objeto de maniobras ilícitas que buscan alterar su integridad. Dichas acciones son ejecutadas por actores con habilidades especializadas, conocidos como hackers, quienes utilizan técnicas sofisticadas para infiltrarse en los sistemas. Al considerar la información como el recurso más preciado de una organización, se han implementado variadas estrategias para intensificar la protección de los datos. Esto incluye la instauración de normativas y procedimientos diseñados para asegurar una barrera efectiva contra cualquier esfuerzo de compromiso (Ovallos et al., 2020).

En el contexto de la seguridad de las redes de área local (LAN), la práctica más común se relaciona a que un administrador asume la responsabilidad de implementar medidas de seguridad como la instalación de cortafuegos y programas antivirus, donde el resto de los usuarios no asumen esta responsabilidad y subestima el impacto que cada uno de ellos sobre la seguridad general de la red. Por ejemplo, una configuración de un cortafuego pierde efectividad si un usuario compromete la red al acceder a Internet mediante conexiones alternativas no seguras, como la utilización de una red Wi-Fi pública a través de un dispositivo personal. Este comportamiento abre puertas a amenazas como gusanos o troyanos, que podrían infiltrarse y lanzar ataques desde dentro de la red (Carballar, 2021).

Por otra parte, con la difusión de la Inteligencia Artificial (IA) se ha marcado una evolución en diversos sectores de la sociedad, ya que, esta ha reducido el esfuerzo, tiempo y costo asociado a ciertas actividades manuales. Los objetivos de la IA se han expandido, como es en el ámbito de la ciberseguridad. Ante la creciente diversidad de los ciberataques, las diferentes herramientas de IA han llegado a ser aliados para detectar y, en ocasiones, neutralizar estas amenazas. No obstante, existe la paradoja de que, mientras la IA se erige

como un elementos en contra las incursiones digitales, también posee el potencial de facilitar la perpetración de estos ataques (Bardají, 2022).

En efecto, los riesgos asociados con la inteligencia artificial (IA) y el big data figuran entre las principales preocupaciones sobre el manejo de datos personales y su privacidad, con el riesgo de la suplantación de identidad. Las acciones realizadas por las herramientas IA como deducir, predecir y monitorear patrones de comportamiento, suscitan serias preocupaciones debido a que estos sistemas suelen depender de bases de datos con sesgos, lo que puede resultar en decisiones erróneas y contrarias a las necesidades de la seguridad (OHCHR, 2021).

Como se ha mencionado, el uso de la IA en la detección de vulnerabilidades de sistemas informáticos ha hecho uso de distintas estrategias de aprendizaje automático, tales como: técnicas de aprendizaje supervisado y no supervisado, como la regresión logística y el clustering, donde se identifican patrones de vulnerabilidad en el código fuente, sin necesidad de datos etiquetados previamente. Se pueden analizar registros de eventos y metadatos para detectar anomalías sospechosas. Además, el aprendizaje por refuerzo y las redes generativas adversarias (GAN) contribuyen a simular escenarios de ciberataques, permitiendo a los sistemas de IA aprender a identificar y prevenir de manera más eficiente las vulnerabilidades potenciales (3digits, 2019).

1.2. Proceso investigativo metodológico

El proceso metodológico tendrá un enfoque cuantitativo, para el cual se aplicó una encuesta a una muestra a conveniencia de profesionales de TI y se la seguridad informática. A continuación se detallan las actividades que involucro este proceso:

Definición de objetivos de la encuesta: Para este proyecto, los objetivos podrían incluir determinar el nivel de conciencia sobre las vulnerabilidades de seguridad en redes de área local, evaluar la eficacia de las herramientas de seguridad actuales, y comprender cómo la integración de la inteligencia artificial puede mejorar los protocolos de seguridad.

Revisión de literatura: Se realizará un análisis de la literatura existente sobre inteligencia artificial aplicada al análisis de vulnerabilidades en seguridad informática. Esta revisión ayudará a establecer un marco conceptual, permitiendo comprender las tendencias emergentes de la IA en el ámbito de la ciberseguridad.

Identificación de población y muestra: La población objetivo de la encuesta se compone de profesionales de TI y seguridad que administran redes de área local. La muestra será seleccionada, fue realizada a conveniencia, con profesionales y

colegas encargados de la gestión informática, de redes y ciberseguridad en sus respectivas empresas.

Diseño de la encuesta: El diseño incluye preguntas cerradas que se alineen directamente con los objetivos de la investigación. Estas preguntas evaluarán aspectos como la percepción actual de la amenaza, la utilización de herramientas de IA y la disposición a adoptar nuevas tecnologías.

Validación del cuestionario: Antes de su implementación, el cuestionario será validado para asegurar su fiabilidad y validez. Esto incluirá revisiones por expertos en el tema de seguridad informática.

Recopilación de datos: la encuesta será administrada mediante formularios electrónicos, en este caso Google Forms, para maximizar la tasa de respuesta, la calidad de los datos, y la rapidez en su procesamiento.

Análisis de datos: Los datos recopilados serán analizados mediante estadísticos descriptivos para identificar patrones en la adopción de IA en la seguridad informática.

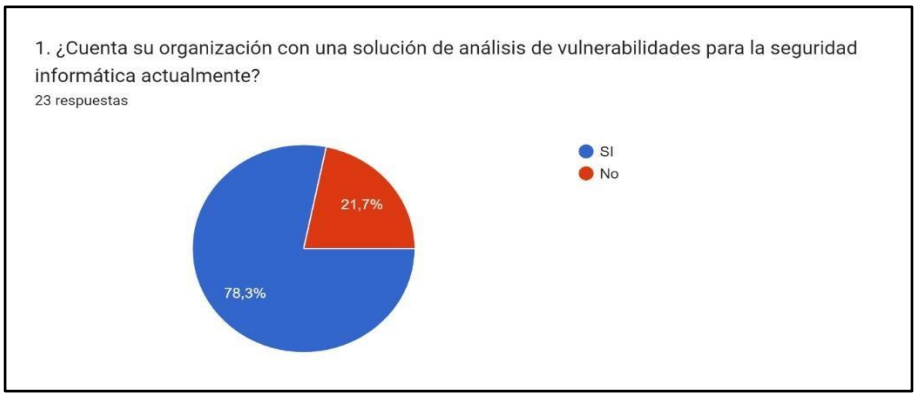
Implementación de resultados: los resultados del análisis se interpretarán en relación con los objetivos de la investigación. Se discutirán las implicaciones prácticas de los hallazgos, proporcionando una base para el desarrollo de recomendaciones estratégicas para la implementación efectiva de soluciones de IA en el análisis de vulnerabilidades de redes de área local.

1.3. Análisis de resultados

A continuación se presentan los resultados de la encuesta aplicada (ver Anexo 1) a una muestra de profesionales de TI y seguridad de la información. En la Figura 1 se muestran los resultados de la pregunta 1.

Figura 1

Respuestas pregunta 1 de la encuesta

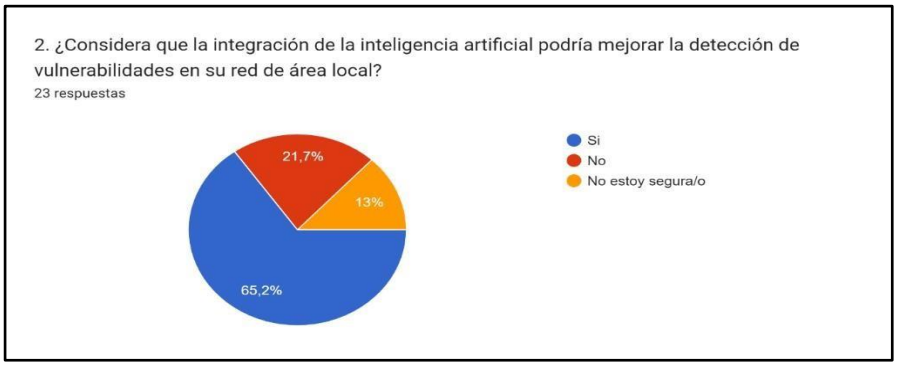


Nota: Elaboración propia.

Los resultados de la pregunta 1 indican que el 78.3% de las organizaciones encuestadas (sus profesionales en TI) carecen de una solución de análisis de vulnerabilidades actualizada, evidenciando un déficit en la infraestructura de seguridad cibernética. Este vacío en la adopción de herramientas muestra una oportunidad para la implementación de sistemas basados en IA, capaces de mejorar la identificación y gestión de amenazas en tiempo real. A continuación en la figura 2 se muestran los resultados de la pregunta 2 de la encuesta.

Figura 2

Respuestas pregunta 2 de la encuesta

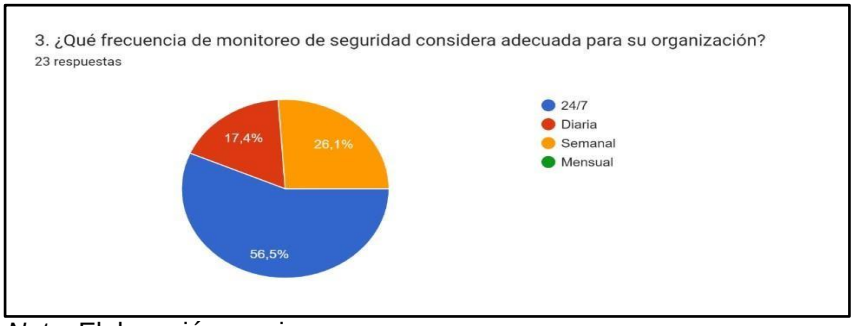


Nota: Elaboración propia.

Dentro de la muestra de profesionales de TI, un 65.2% reconoce el potencial de la inteligencia artificial para la detección de vulnerabilidades en redes LAN, mostrando una percepción favorable hacia la integración de tecnologías de IA en la seguridad informática. Un 21.7% no está seguro, lo que podría indicar una falta de familiaridad con las aplicaciones de IA o una incertidumbre sobre su efectividad. Solamente un 13% no ve beneficios en la incorporación de IA, lo cual resalta la necesidad de demostraciones prácticas o casos de estudio que evidencien su efectividad en este campo. A continuación en la figura 3 se muestran los resultados de la pregunta 3 de la encuesta.

Figura 3

Respuestas pregunta 3 de la encuesta



Nota: Elaboración propia.

La mayoría de los profesionales de TI encuestados (56.5%) perciben el monitoreo de seguridad 24/7 como la frecuencia óptima para sus organizaciones, enfatizando la vigilancia continua y la capacidad de respuesta inmediata ante incidentes de seguridad. El 26.1% prefiere un monitoreo diario, lo que indica una supervisión regular, mientras que las preferencias por el monitoreo semanal y mensual son significativamente menores (17.4% y 0% respectivamente). A continuación en la figura 4 se muestran los resultados de la pregunta 4 de la encuesta.

Figura 4

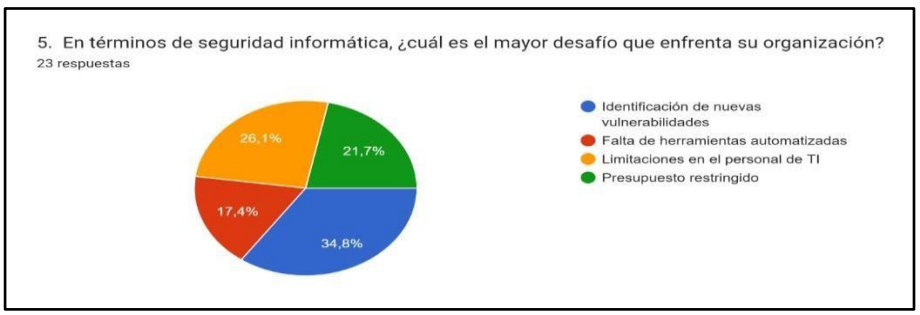
Respuestas pregunta 4 de la encuesta

Nota: Elaboración propia.

Un 26.1% de las organizaciones encuestadas han experimentado una violación de seguridad en el último año, que muestra la existencia de vulnerabilidades en las prácticas de seguridad actuales. El 73.9% restante no reportó incidentes, lo que podría indicar una efectividad en las medidas de protección implementadas o una falta de detección o reporte adecuado. Esta información resalta la necesidad de mejorar las estrategias de seguridad y la importancia de adoptar sistemas avanzados de detección de intrusos y análisis de vulnerabilidades A continuación en la figura 5 se muestran los resultados de la pregunta 5 de la encuesta.

Figura 5

Respuestas pregunta 5 de la encuesta

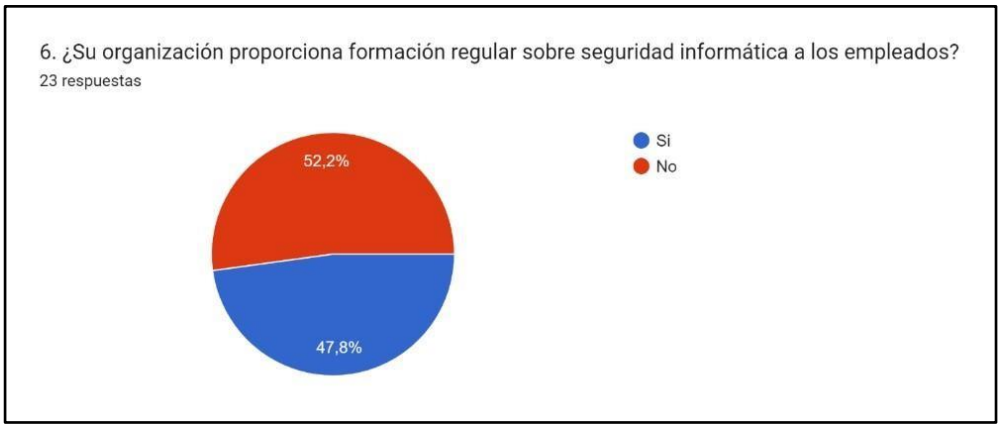


Nota: Elaboración propia.

El principal desafío en seguridad informática, para el 34.8% de los encuestados, es la identificación de nuevas vulnerabilidades. El 26.1% señala la falta de herramientas automatizadas como un obstáculo, que demuestra una brecha en la optimización de procesos de seguridad. Además, el 21.7% menciona limitaciones en el personal de TI, y el 17.4% reporta el presupuesto restringido como barreras, lo que resalta la importancia de recursos humanos capacitados y financiación adecuada para una gestión efectiva de la seguridad informática. A continuación en la figura 6 se muestran los resultados de la pregunta 6 de la encuesta.

Figura 6

Respuestas pregunta 6 de la encuesta

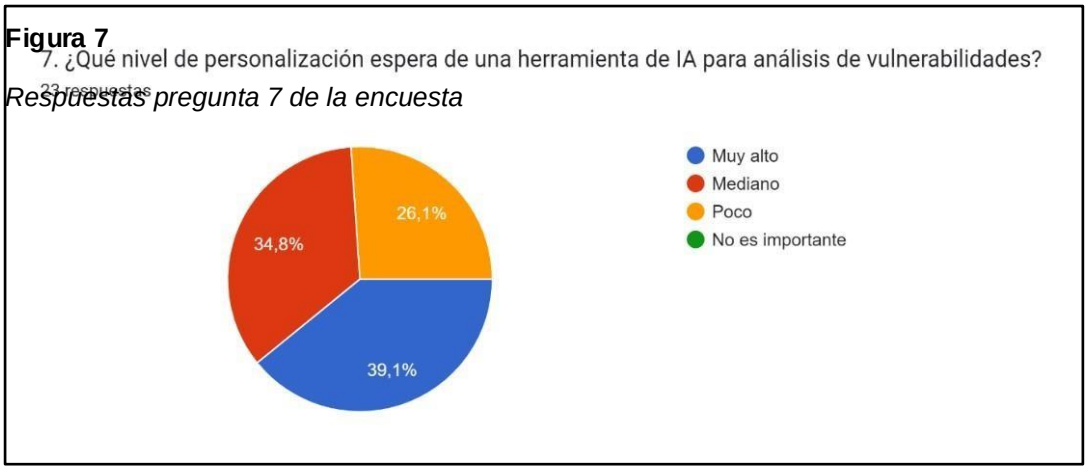


Nota: Elaboración propia.

Sobre la formación de seguridad informática, distribución casi equitativa en las respuestas muestra que el 52.2% de las organizaciones encuestadas brindan formación regular en seguridad informática a sus empleados, lo que indica la importancia del factor humano en la mitigación de riesgos cibernéticos. Por otro lado, el 47.8% que no proporciona dicha formación, que evidencia que están expuesto a mayores riesgos por errores humanos, siendo esta un área clave en el diseño de las estrategias de seguridad cibernética. A continuación en la figura 7 se muestran los resultados de la pregunta 7 de la encuesta.

Figura 7

Respuestas pregunta 7 de la encuesta

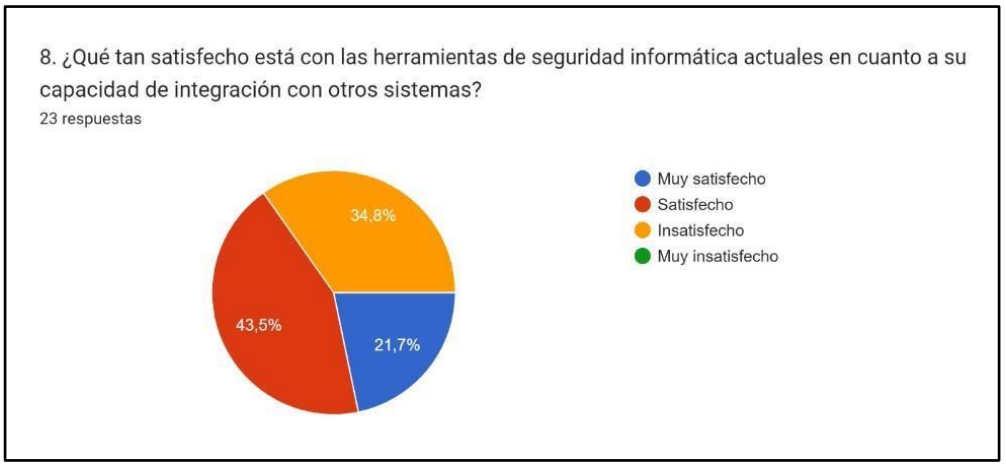


Nota: Elaboración propia.

La mayoría de los profesionales de TI (39.1%) esperan un alto nivel de personalización en herramientas de IA para el análisis de vulnerabilidades, es decir, ajustarse a las necesidades de infraestructuras de seguridad específicas de cada organización. Un 34.8% considera suficiente un nivel de personalización mediano, mostrando una preferencia por soluciones más genéricas pero aún configurables. Solo el 26.1% se conformaría con poca o ninguna personalización, lo que indica que, mientras algunos entornos pueden operar con soluciones estándar. A continuación en la figura 8 se muestran los resultados de la pregunta 8 de la encuesta.

Figura 8

Respuestas pregunta 8 de la encuesta



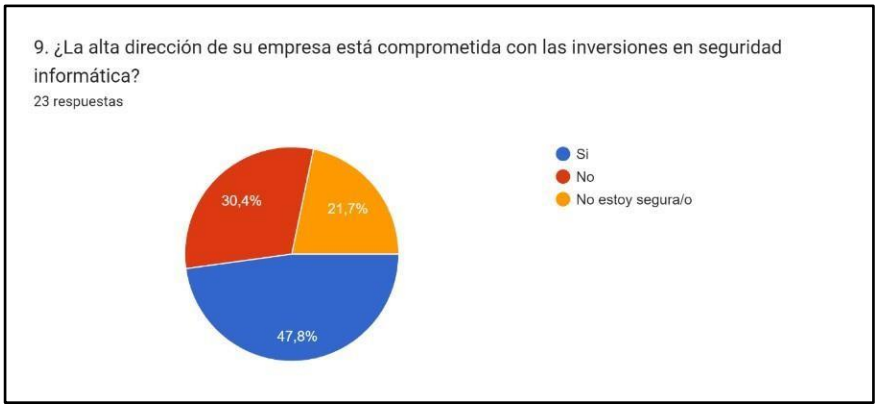
Nota: Elaboración propia.

El 43.5% de los encuestados se siente satisfecho con la capacidad de integración de las herramientas de seguridad informática actuales con otros sistemas. Sin embargo, un 34.8% se muestra insatisfecho y un 21.7% muy insatisfecho, lo que colectivamente representa una significativa demanda de mejoras en la interoperabilidad de las plataformas

de seguridad. Esto pone en evidencia la importancia de desarrollar soluciones de IA que ofrezcan una integración más fluida y versátil con los diversos sistemas operativos y aplicaciones tecnológicas empresariales. A continuación en la figura 9 se muestran los resultados de la pregunta 9 de la encuesta.

Figura 9

Respuestas pregunta 9 de la encuesta

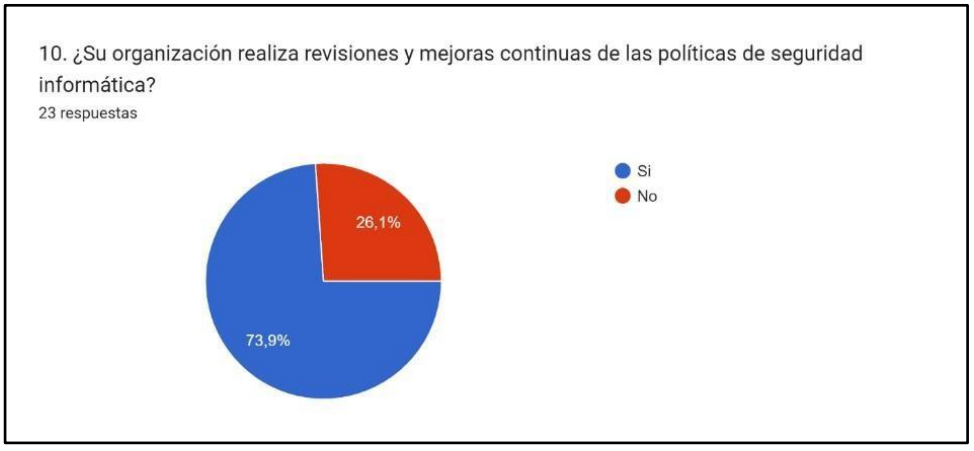


Nota: Elaboración propia.

Aproximadamente la mitad de los profesionales de TI (47.8%) afirman que la alta dirección de sus empresas está comprometida con las inversiones en seguridad informática. Sin embargo, un 30.4% de los encuestados percibe falta de compromiso en la inversión, y un 21.7% no está seguro de la posición de la dirección, lo que señala una oportunidad para mejorar el entendimiento entre los ejecutivos y los departamentos de TI sobre la importancia de la ciberseguridad. A continuación en la figura 10 se muestran los resultados de la pregunta 10 de la encuesta.

Figura 10

Respuestas pregunta 10 de la encuesta



Nota: Elaboración propia.

Un 73.9% de los encuestados confirma que sus organizaciones llevan a cabo revisiones y mejoras continuas de las políticas de seguridad informática. Sin embargo, el 26.1% restante que no realiza este proceso de actualización constante está en riesgo de sufrir brechas de seguridad debido a políticas obsoletas o inadecuadas, lo que muestra la necesidad de un enfoque proactivo en la gestión de la seguridad informática.

CAPÍTULO II: PROPUESTA

2.1 Fundamentos teóricos aplicados

La seguridad informática comprende una serie de estrategias y prácticas destinadas a proteger los sistemas informáticos, asegurando que se utilicen adecuadamente y sin interferencias externas no autorizadas (Miranda, 2019). Sus principios fundamentales son:

- Confidencialidad: es restricción de acceso a la información solo a entidades autorizadas para preservar su privacidad.
- Integridad: implica mantener la precisión y totalidad de la información almacenada en los sistemas.
- Disponibilidad: asegura que la información sea accesible para los usuarios autorizados cuando se requiera.

La protección de la información implica medidas preventivas para defender la confidencialidad, integridad y disponibilidad de la información, de forma independiente de su formato o medio. Esto requiere que las organizaciones implementen y ajusten continuamente métodos eficaces para la protección de datos y para sostener una infraestructura tecnológica robusta que garantice la custodia segura de la información (Miranda, 2019).

En el ámbito de la seguridad, tanto digital como en general, los términos vulnerabilidad, amenaza y riesgo están intrínsecamente conectados, como se muestran a continuación (AMBIT-BST, 2023):

- Vulnerabilidad informática, representa las condiciones inherentes a un sistema que lo hacen propenso a ser explotado por una amenaza, siendo una indicación de la capacidad de un sistema para responder ante la posible ocurrencia de un incidente adverso, ya sea por factores internos o externos. Estas vulnerabilidades pueden poner en peligro activos informáticos y datos ante un ataque potencial.
- Amenaza informática, es la posibilidad de un evento perjudicial, en cualquier momento, que puede generar pérdidas tangibles o intangibles de los recursos de TI y los sistemas de información. Dichas amenazas abarcan acciones malintencionadas de individuos dentro o fuera de una organización que buscan dañar la infraestructura tecnológica y la información que se procesa y transmite.
- Riesgo informático se refiere a los problemas latentes que podrían materializarse y afectar los sistemas de información o el hardware si no se establecen medidas de protección eficaces contra las mencionadas vulnerabilidades y amenazas.

2.1.1 Riesgos de la seguridad en los sistemas de información:

Se han detectado varios problemas y limitaciones en la evaluación del riesgo de seguridad de la información, tales como (Azan et al., 2018):

- Divergencias en los niveles de habilidad entre los profesionales al usar listas de chequeo para evaluar los sistemas de gestión de bases de datos (SGBD), lo que puede llevar a discrepancias entre el riesgo de seguridad de la información (RSI) evaluado y el previamente diagnosticado.
- La clasificación del RSI en los SGBD se categoriza de manera general como Alto, Medio o Bajo, resultando en una medida que puede ser ambigua y carecer de precisión, dependiendo del tipo de aplicación, la empresa o los criterios utilizados.
- El tiempo requerido por muchos profesionales para entregar los resultados de la evaluación del RSI puede extenderse por horas o incluso días, lo que retrasa el proceso de toma de decisiones, subrayando la necesidad de explorar métodos alternativos que faciliten evaluaciones rápidas y la generación de soluciones en tiempo oportuno.

2.1.2 Tipos de ataques dentro de un entorno informático

En la Tabla 1 muestra los diferentes ataques que pueden ocurrir dentro de un entorno informático, detallando su naturaleza, método y objetivo (Wazid et al., 2022):

Tabla 1

Ataques dentro de un entorno informático

Tipo de Ataque	Naturaleza	Método	Objetivo
Escuchando a escondidas	Pasiva	Ataque de olfateo o espionaje	Escuchar conversaciones secretas
Análisis de tráfico	Pasiva	Interceptación y análisis de mensajes	Obtener información sobre la conversación, patrones y ubicación
Ataque de repetición	Activa	Retransmisión de mensajes capturados	Engañar o desviar al destinatario
Hombre en el medio (MiTM)	Activa	Conexiones independientes con entidades	Interceptación, modificación o inserción de información
Suplantación de identidad	Activa	Imitación de una parte legítima	Transmisión de mensajes modificados o nuevos
Denegación de servicio (DoS/DDoS)	Activa	Envío de múltiples solicitudes falsas	Inundar los recursos informáticos, impidiendo el servicio a usuarios legítimos

Ataque de malware	Activa	Ejecución de scripts maliciosos	Realizar actividades no autorizadas como robo de datos o cifrado ilegal
Ataque de scripting	Activa	Divulgación de información de bases de datos	Obtener información secreta como contraseñas y detalles de tarjetas
Ataque interno privilegiado	Activa	Acceso a información de registro por usuario privilegiado	Difícil de defender y de alto impacto adverso
Robo físico de dispositivos inteligentes	Activa	Extracción de información sensible mediante análisis de poder	Realización de tareas no autorizadas
Ataque de cumpleaños	Criptográfico	Aprovechamiento de las matemáticas detrás del problema del cumpleaños	Adivinación de credenciales
Ataque de diccionario	Criptográfico	Escritura sistemática de cada palabra de un diccionario como contraseña	Violación de la seguridad del sistema
Ataque de verificador robado	Activa	Robo de dispositivos y análisis de energía	Extracción de información confidencial
Cómputo de clave de sesión no autorizado	Activa	Cálculo de la clave de sesión entre entidades legítimas	Acceso no autorizado a la comunicación
Ataques a modelos de aprendizaje automático	Activa	Métodos diversos para invadir datos de entrenamiento y prueba	Afectar el funcionamiento normal de la tarea de ML

Nota: Adaptado de (Wazid et al., 2022).

2.1.3 Riesgo y vulnerabilidades en una LAN

La seguridad dentro de las redes de área local (LAN) se centra en identificar y comprender las debilidades más significativas, desde el spoofing de direcciones IP hasta ataques de denegación de servicio y problemas de implementación que comprometen la integridad de los datos y la privacidad de los usuarios. Profundizar en estas vulnerabilidades es esencial para desarrollar estrategias efectivas de mitigación y protección.

En las redes de área local (LAN), Ethernet destaca como la más prevalente en entornos cableados, ofreciendo la capacidad de formar redes de considerable extensión y alta velocidad de transmisión. Esta tecnología se basa en el uso de direcciones físicas o MAC, únicas a nivel global y asignadas por el fabricante, para la identificación de dispositivos dentro de la red. Por lo tanto, se puede esperar que los que datos se transmiten en frames y que pueden contener hasta 1.500 bytes de datos. Para la interconexión de una red Ethernet con otras redes o Internet, se emplea el protocolo ARP (protocolo de resolución de direcciones)

para la conversión entre direcciones físicas e IP (Miranda, 2019). A pesar de los avances y la evolución de Ethernet, aún enfrenta vulnerabilidades como las que se detallan a continuación en la Tabla 2.

Tabla 2

Ataques dentro de un entorno informático

Vulnerabilidad	Descripción
Sniffers de Ethernet	Originalmente, Ethernet facilitaba la captura de tráfico por cualquier dispositivo en la red debido a su topología de bus y al modo promiscuo en tarjetas de red, lo que permitía espiar el tráfico. Aunque las topologías y conmutadores modernos reducen este riesgo, vulnerabilidades como el MAC flooding pueden degradar conmutadores a actuar como concentradores, revelando todo el tráfico.
Modificación de direcciones MAC	Las direcciones MAC, únicas para cada tarjeta de red, pueden modificarse fácilmente en muchos sistemas operativos, comprometiendo los mecanismos de control de acceso y seguridad basados en MAC, permitiendo la suplantación y evasión de restricciones.
Vulnerabilidades en el protocolo ARP	ARP resuelve direcciones IP a MAC en redes como Ethernet, pero es vulnerable al ARP poisoning, permitiendo ataques de denegación de servicio y de hombre en el medio al insertar entradas falsas en cachés ARP, comprometiendo la comunicación y la seguridad de la red. Soluciones como entradas fijas en la caché ARP y la monitorización de red ayudan a mitigar estos riesgos.

Nota: Adaptado de (Miranda, 2019)

2.1.4 Vulnerabilidades de interconexión de redes

Dada la naturaleza que está relacionada con la interconexión de redes, el número de vulnerabilidades es muy extenso, no obstante en la Tabla 3 se mencionan las más comunes:

Tabla 3

Ataques dentro de un entorno informático

Tipo de Vulnerabilidad	Descripción	Subtipos y Descripciones
Vulnerabilidades en IP	Relacionadas con el protocolo IP, incluyen ataques como IP spoofing y problemas de implementación que pueden	**IP spoofing**: Generación de paquetes IP con direcciones de origen falsas, usado en ataques de denegación de servicio o suplantación de identidad

	causar interrupciones significativas.	**Packet-of-death**: Envío de paquetes IP erróneos que causan fallos en algunas implementaciones, como el land attack **Vulnerabilidades en la fragmentación**: Envío de fragmentos de paquetes erróneos que se sobreponen sobre campos de datos, provocando fallos. Ejemplo: teardrop attack **IP source routing**: Opciones de IP que permiten especificar rutas de retorno, potencialmente usadas para recibir respuestas utilizando IP spoofing.
Vulnerabilidades en ICMP	Asociadas al protocolo ICMP, generalmente vinculadas a ataques de denegación de servicio.	**Ping flooding**: Uso de mensajes echo request para sobrecargar un sistema. **Ping of death**: Envío de paquetes ICMP más grandes de lo permitido, provocando un buffer overflow. **Smurf attack**: Ataques de denegación de servicio usando pings en broadcast con la dirección de origen falsa, provocando respuestas masivas hacia la víctima.
Vulnerabilidades en DNS	Afectan la resolución de nombres de dominio, permitiendo ataques significativos como redirección de tráfico y envenenamiento de caché.	**DNS spoofing**: Emisión de respuestas falsas para alterar la correspondencia entre nombres de dominio e IPs, redirigiendo el tráfico. **DNS cache poisoning**: Introducción de información falsa en la caché de DNS, afectando la resolución de nombres. **DNS amplification attacks**: Ataques que explotan la resolución recursiva de DNS para amplificar el tráfico hacia la víctima, causando denegación de servicio.
Vulnerabilidades en OSPF y BGP	Impactan en los protocolos de encaminamiento como OSPF y BGP, permitiendo la introducción de rutas de encaminamiento falsas.	**Ataques a OSPF**: Posibilitan la inserción de información de encaminamiento errónea, facilitando la denegación de servicio o el aislamiento de partes de la red. **Ataques a BGP** (implícito): Similar a OSPF, afectan la integridad del encaminamiento entre sistemas autónomos, potencialmente desviando tráfico o aislando redes.

Nota: Adaptado de (Miranda, 2019)

2.1.5La inteligencia artificial

La Inteligencia Artificial (IA) se ha reconocido como las destrezas que presentan las máquinas para analizar y solucionar problemas, así como realizar tareas que implican inteligencia. Su aplicación se extiende a numerosas áreas, incluidas la construcción de edificios inteligentes, la protección ambiental, las finanzas y la química, mostrando su versatilidad y capacidad para innovar (Martínez et al., 2023).

La IA a pesar de no tener una definición única, es ampliamente reconocida por su habilidad para ejecutar acciones que demandan inteligencia, como razonar estratégicamente, solucionar problemas complejos y hacer juicios en situaciones inciertas. Además, involucra la representación del conocimiento, incluyendo el sentido común, la planificación, el aprendizaje y la comunicación en lenguaje natural, orientando todas estas habilidades hacia metas compartidas. Se extiende para abarcar la percepción sensorial y la acción en el entorno. La inteligencia artificial también abarca aspectos interdisciplinarios que subrayan la importancia de rasgos adicionales como la creatividad y la autonomía, englobando sistemas que presentan diversas capacidades como la creatividad computacional y la toma automatizada de decisiones. Aunque se han logrado avances considerables, la IA aún no ha alcanzado la plenitud de las capacidades humanas (Teigens et al., s. f.)

2.1.6 Características de la inteligencia artificial

Entre las principales características que se presentan dentro del concepto y aplicaciones de inteligencia artificial están (Scaler, 2024):

- Ingeniería de funciones: este proceso se centra en la selección y transformación de datos brutos en características que mejoren el rendimiento de los modelos de IA. Se destaca la importancia de elegir las características correctas, utilizando algoritmos de selección basados en su relevancia y asegurando su independencia para evitar redundancias. Las técnicas como el proceso de ortogonalización de Gram-Schmidt y el Análisis de Componentes Principales son esenciales tanto para el aprendizaje supervisado como no supervisado, facilitando la conversión de datos brutos en un formato más manejable que potencia la precisión y eficiencia de los modelos.
- Redes Neuronales Artificiales (RNA): están tratan de emular el funcionamiento del cerebro humano y se estructuran en capas de neuronas que procesan y transmiten señales. Se distinguen principalmente en redes feedforward, donde la información se mueve en una sola dirección, y redes recurrentes, que pueden manejar datos secuenciales a través de "memorias" de entradas anteriores. Las RNA son especialmente adecuadas para desentrañar relaciones complejas en datos, con

aplicaciones en marketing, finanzas, detección de fraudes y diagnóstico de enfermedades.

- Aprendizaje profundo: Este avance en el aprendizaje automático permite a las máquinas "pensar" de manera similar a los humanos mediante el uso de redes con múltiples capas ocultas, lo que les otorga la capacidad de realizar tareas complejas de clasificación y reconocimiento sin intervención humana directa. La arquitectura de aprendizaje profundo aprovecha la potencia de unidades de procesamiento gráfico (GPU) para manejar eficientemente grandes volúmenes de datos y complejidades computacionales, encontrando aplicaciones en visión por computadora, reconocimiento de voz, y más.

2.1.7 Modelos de inteligencia artificial

Un modelo de inteligencia artificial (IA) se caracteriza por su habilidad para tomar decisiones autónomas sin necesidad de imitar la inteligencia humana. Los primeros éxitos en IA se dieron en juegos como las damas y el ajedrez en la década de 1950, con modelos que respondían activamente a las jugadas del adversario humano. Los modelos de IA son particularmente efectivos en tareas o ámbitos específicos donde su enfoque de toma de decisiones destaca. Los sistemas avanzados a menudo combinan múltiples modelos de IA, utilizando estrategias de aprendizaje colectivo como el embolsado y el impulso (IBM, 2022).

Los modelos de inteligencia artificial (IA) están diseñados para tomar decisiones de forma automatizada. Sin embargo, solo aquellos con capacidades de aprendizaje automático (Machine Learning ML) pueden mejorar su desempeño de manera autónoma a lo largo del tiempo, adaptándose y optimizando su rendimiento basado en nuevos datos y experiencias. Aunque el aprendizaje automático es una forma de IA, no todos los sistemas de IA emplean ML. Los enfoques de IA más básicos se basan en reglas lógicas predeterminadas, como los sistemas de reglas "si-entonces", también conocidos como motores de reglas, sistemas expertos o IA simbólica, que requieren la definición explícita de sus operaciones por parte de los desarrolladores (IBM, 2022).

El aprendizaje automático (ML) tiene 3 elementos de aprendizaje especifico: supervisado, no supervisado y por refuerzo. Cada categoría tiene su metodología y aplicación específicas en la inteligencia artificial. A continuación, la Tabla 4 muestra las diferentes características relacionadas con cada tipo de aprendizaje de ML:

Tabla 4

Ataques dentro de un entorno informático

Categoría	Descripción	Características Principales
Aprendizaje Supervisado	Conocido como aprendizaje automático "clásico", se basa en datos etiquetados por humanos.	Requiere etiquetado manual por expertos. Utiliza etiquetas para inferir características de los datos. Ejemplo: modelos de reconocimiento de imágenes.
Aprendizaje No Supervisado	Detecta patrones sin necesidad de etiquetas o intervención externa.	No requiere etiquetas. Agrupa datos según patrones detectados. Ejemplo: sistemas de recomendación.
Aprendizaje por Refuerzo	Aprende por medio de prueba y error, a través de recompensas o penalizaciones.	Se basa en la recompensa sistemática. Aplica en sugerencias de redes sociales y vehículos autónomos.

Nota: Adaptado de (Wazid et al., 2022).

La investigación ha evidenciado un aprendizaje profundo, un avance más evolucionado del aprendizaje no supervisado, utiliza redes neuronales para imitar el funcionamiento cerebral y puede realizar tareas complejas, esto debido a su alta capacidad de procesamiento de grandes volúmenes de información, aunque requiere significativos recursos computacionales.

2.1.8 Inteligencia artificial y la seguridad de la información

Como se mencionó en el apartado de la seguridad informática esta fundamenta en tres pilares esenciales: confidencialidad, integridad y disponibilidad, que son necesarios para las organizaciones debido al valor incalculable de la información. En este sentido, la inteligencia artificial (IA) se ha convertido en un elemento clave dentro del análisis de seguridad, implementando soluciones ante la detección de intrusos y el filtrado de spam. Además, los sistemas expertos de IA, que emulan el razonamiento humano, necesitan mantenimientos periódicos para un rendimiento óptimo. Estos sistemas avanzan a través del aprendizaje automático y teorías conexionistas, analizando datos para validar su eficacia en aplicaciones del mundo real (Torres y Rendón, 2020).

Dentro de las aplicaciones que se han desarrollado diferentes herramientas de inteligencia artificial, están los sistemas detectores de intrusos IDS, la detección de correos no deseados y otras aplicaciones, como se muestran a continuación

1) Sistemas detectores de intrusos IDS

Dentro de la detección de intrusos las técnicas de Inteligencia Artificial (IA) desempeñan han pemitido optimizar y detectar eficazmente las intrusiones, reduciendo así la carga de trabajo humano. La aplicación de métodos de IA en IDS abarca desde el uso de Sistemas Basados en Casos (CBS) con herramientas como Snort, mejorando las alertas y falencias de seguridad, hasta técnicas avanzadas como Máquinas de Vectores de Soporte (SVMs), Redes Neuronales Artificiales (ANNs), y más (Hernández, 2013). Los estudios sobre este tema indican:

- Programas genéticos lineales (LPGs) son más eficientes en detección precisa, a pesar del tiempo que requieren.
- La regresión multivariada adaptativa con splines (MARS) supera a las SVMs en clasificar ataques graves como accesos no autorizados.
- Las SVMs ofrecen una mejor escalabilidad y rapidez en comparación con las ANNs, especialmente con grandes volúmenes de datos.

2) Correo no deseado (Spam)

El problema del correo spam ha crecido, consumiendo excesivos recursos computacionales y eludiendo las aplicaciones anti-spam. Las técnicas de Inteligencia Artificial son una solución eficaz, que mediante herramientas analíticas avanzadas, como el modelado formal para información incompleta, se han utilizado para generar reglas y analizar datos. Entre los diferentes modelos inteligentes de detección y filtrado de spam, destacan métodos como Naïve Bayes y sus variantes, las Máquinas de Vectores de Soporte (SVM), y otras técnicas de reconocimiento de patrones y razonamiento basado en casos, que han probado ser exitosas y adaptativas para enfrentar el spam (Hernández, 2013).

3) Antivirus

El uso de la Inteligencia Artificial para desarrollar aplicaciones de antivirus se ha centrado en el aprendizaje de sistemas para identificar virus metamórficos. Además, se ha estudiado el uso de Redes Neuronales Artificiales para detectar gusanos informáticos en sistemas operativos Windows, aprovechando su habilidad para reconocer patrones en escenarios complejos y realizar clasificaciones rápidas(Hernández, 2013). Las técnicas de IA utilizadas en la detección de virus incluyen:

- Minería de Datos.
- Redes Neuronales
- Tecnología Agente.
- Tecnología Artificial Inmune.
- Tecnología heurística

Por su parte Ramasubramanian et al. (2021) menciona internet es una fuente principal de generación de datos, tanto directa como indirectamente. La transmisión de datos a través de redes puede ser un vector para ciberdelitos, lo que aumenta la importancia de la ciberseguridad. En este sentido la IA es clave para reducir los ataques cibernéticos, facilitando la detección de malware con base en datos de ataques previos, con aplicaciones relacionadas con:

a) Sistemas expertos en ciberseguridad: estas herramientas o paquetes de software de IA aportan el conocimiento necesario a los usuarios o a otros sistemas, incorporando la sabiduría de expertos en el tema.
b) Aplicaciones de aprendizaje profundo en Ciberseguridad: la escasez de datos desagregados es un problema común en la investigación de la ciberseguridad. A menudo se atribuye a la necesidad de confidencialidad, pero incluso en grandes empresas con recursos internos, la información sobre amenazas puede ser difícil de transformar en conjuntos de datos categorizados adecuados para el aprendizaje automático.
c) Aplicaciones del aprendizaje automático en ciberseguridad: las amenazas a la ciberseguridad cambian y se desarrollan constantemente, requiriendo una respuesta automática e inmediata. Por lo tanto, la aplicación de métodos como el aprendizaje profundo, que no precisan de conocimientos previos ni se basan en clasificaciones realizadas por expertos, permiten desarrollo estrategias de inteligencia artificial en el ámbito de la ciberseguridad.
d) Aplicaciones de Minería de Datos en Ciberseguridad: La minería de datos busca patrones y tendencias significativas en grandes bases de datos. Esta técnica recopila conocimientos útiles e identifica patrones ocultos en conjuntos de datos extensos, inaccesibles mediante enfoques computacionales. Involucra aprendizaje automático, bases de datos, análisis, sistemas expertos, visualización, cálculo de alto rendimiento, conjuntos aproximados, redes neuronales y representación de la información, utilizando diferentes métodos como agrupación, análisis de relaciones, modelos de regresión y análisis de secuencias para apoyar la minería de datos.

2.1.9Riesgos de la IA en la seguridad de sistemas informáticos

Los riesgos de la IA deberían verse como extensiones de los riesgos asociados con las tecnologías digitales no basadas en IA, a menos que se demuestre lo contrario, y deberían enmarcarse como extensiones del trabajo para gestionar otros riesgos digitales. En efecto, durante mucho tiempo la IA ha sido tratada como si estuviera fuera de los marcos legales existentes relacionado con la gestión y medidas de ciberseguridad. Si la IA no se menciona específicamente en las iniciativas de divulgación y gestión de vulnerabilidades y otras

actividades de ciberseguridad, muchos pueden no darse cuenta de que está incluida. Es decir, se deben ver a los modelos de IA como otro tipo de software, sujeto a vulnerabilidades y merecedor de una alta atención de ciberseguridad.(Dempsey, 2021).

Las IA están expuestas a entidades maliciosas, incluidos los atacantes en línea, buscan constantemente explotar vulnerabilidades a través de una variedad de ataques, lo que ha llevado a proponer diversos protocolos de seguridad para mitigar estas amenazas. Estos protocolos se han clasificado en diferentes categorías, tales como: autenticación, control de acceso, detección de intrusiones, administración de claves y seguridad habilitada para blockchain. Cada uno de estos aborda aspectos específicos de la ciberseguridad, desde verificar la autenticidad de usuarios y dispositivos hasta prevenir el acceso no autorizado y detectar intrusiones maliciosas (Wazid et al., 2022). A continuación, en la Tabla 5 se presenta un resumen de estos protocolos y sus características en formato de tabla:

Tabla 5

Protocolos para evitar riesgos en la IA

Categoría de Protocolo	Descripción	Características
Protocolos de Autenticación	Verificación de la autenticidad de alguien o algún dispositivo mediante credenciales o factores asociados.	Autenticación de usuario a usuario Autenticación de usuario a dispositivo Autenticación de dispositivo a dispositivo Protocolos de un factor, dos factores y tres factores
Protocolos de Control de Acceso	Imposición de restricciones al acceso no autorizado de usuarios o dispositivos.	Control de acceso de usuarios Control de acceso de dispositivos Basado en certificados o sin certificados
Protocolos de Detección de Intrusiones	Identificación de entidades maliciosas con intenciones dañinas.	Detección basada en; firmas; anomalías; híbrida; en aprendizaje automático
Protocolos de Gestión de Claves	Gestión segura de claves entre distintas entidades.	Registro por autoridad confiable Generación, almacenamiento, establecimiento y revocación de claves
Protocolos de Seguridad Habilitados para Blockchain	Defensa contra ciberataques mediante el uso de tecnología blockchain.	Datos mantenidos en bloques encadenados con valores hash Tecnología de libro mayor distribuido (DLT)

Nota: Adaptado de (Wazid et al., 2022).

2.1.10 Ventajas de los modelos aprendizaje automático en la ciberseguridad

De acuerdo a Wazid et al. (2022) entre las ventajas que tiene los modelos de aprendizaje automático están:

- Los modelos de aprendizaje automático (ML), susceptibles a distintos ataques, pueden verse salvaguardados mediante la implementación de mecanismos de ciberseguridad específicos. Esto asegura la integridad del funcionamiento, el rendimiento y los datos de entrada, garantizando así predicciones y resultados precisos.
- La incorporación de algoritmos de ML en sistemas de seguridad cibernética, como los sistemas de detección de intrusiones, mejora su eficacia, aumentando la precisión y la tasa de detección mientras reduce la incidencia de falsos positivos,
- La aplicación de modelos de ML en la seguridad cibernética se ha mostrado efectiva para identificar ataques de día cero, gracias a su capacidad para analizar y comparar patrones de comportamiento y características de programas maliciosos, permitiendo una detección automatizada y eficiente.
- La integración de la ciberseguridad con el ML minimiza la dependencia de la intervención humana, ya que la mayoría de las tareas de detección y respuesta ante amenazas pueden ser automatizadas mediante modelos de ML, agilizando las operaciones de seguridad.
- Los sistemas de detección de intrusiones potenciados por ML destacan por su eficiencia y rapidez en la identificación de ataques, así como en la respuesta inmediata ante posibles intrusiones, siempre que se elija el algoritmo de ML más adecuado para cada situación específica (Wazid et al., 2022).

2.1.11Problemas y desafíos del IA en ciberseguridad

La integración de la ciberseguridad con el aprendizaje automático, si bien promete significativas ventajas, enfrenta también una serie de desafíos críticos que deben ser cuidadosamente abordados (Wazid et al., 2022):

Problemas de compatibilidad: la combinación de algoritmos de seguridad (como cifrado, generación y verificación de firmas, hash) con algoritmos de aprendizaje automático puede generar incompatibilidades, especialmente cuando los datos provienen de diversas fuentes, como dispositivos IoT con diferentes técnicas de comunicación.

Sobrecarga: la implementación simultánea de múltiples algoritmos exige recursos adicionales, lo que puede sobrecargar el sistema afectando su operatividad. Por lo

que, se requiere aplicar algoritmos eficientes que optimicen el uso de los recursos sin comprometer las tareas esenciales del sistema.

Precisión: el empleo de modelos de aprendizaje automático depende de la calidad de los conjuntos de datos. Errores en los datos o en la configuración de los modelos pueden conducir a predicciones inexactas, afectando la efectividad de las decisiones basadas en estos modelos.

Defectos en los mecanismos de seguridad: vulnerabilidades no detectadas, poniendo en riesgo la confidencialidad, integridad y disponibilidad de los sistemas. Es crucial realizar pruebas exhaustivas de los protocolos de seguridad para asegurar su robustez frente a ataques potenciales.

2.2 Descripción de la propuesta

La propuesta surge a raíz del incremento de amenazas informáticas y tiene como finalidad presentar recomendaciones para el uso de inteligencia artificial (IA) como herramienta en el análisis y detección de vulnerabilidades dentro de redes LAN. Por lo que, no solo se buscará identificar las brechas de seguridad existentes, sino también prever y neutralizar posibles elementos de ataque antes de que sean explotados. En el presente plan se dará atención a las técnicas de aprendizaje automático y otras herramientas que permitan predecir de forma óptima y efectiva las vulnerabilidades de la infraestructura de las redes LAN.

Estructura general

La propuesta presentada, se desarrollara según el diagrama que se presenta a continuación donde se detallan las fases de la misma como se muestran en la Figura 11.

Figura 11

Estructura General de las fases de la propuesta.

Nota: *Elaboración propia.*

Explicación del aporte

El aporte de la propuesta del Análisis de Vulnerabilidades basado en Técnicas de Inteligencia Artificial para la Seguridad Informática en Redes de Área Local. radica en varios aspectos clave que se detallan a continuación:

Evaluación inicial y definición de requisito

La evaluación inicial y definición de requisitos constituyen la etapa fundacional en el proceso de fortalecimiento de la ciberseguridad, mediante la cual se realiza un inventario de la infraestructura de red LAN actual, identificando dispositivos, sistemas, y aplicaciones críticas. Paralelamente, se definen los requisitos de seguridad, basados en la naturaleza de los datos y las necesidades de protección, los cuales establecen el marco de seguridad informática orientada a la prevención de vulnerabilidades. Las actividades a seguir serían las siguientes:

A) Auditoría de la infraestructura actual: implica realizar un inventario completo de la infraestructura de la red LAN, incluyendo dispositivos, sistemas operativos y aplicaciones en uso. En la tabla 6 se muestran los criterios que a seguir (tomando como base algunas recomendaciones de la ISO/IEC 27001).

Tabla 6

Fase 1 Auditoria de infraestructura actual

Elemento	Descripción	Criterios ISO/IEC 27001
Dispositivos de Red	Inventario de dispositivos de red (routers, switches, firewalls, etc.).	Identificación, clasificación de activos y gestión de activos.
Sistemas Operativos	Listado de sistemas operativos en uso dentro de la red LAN.	Registro de versiones, parches y configuraciones seguras.
Aplicaciones	Inventario de aplicaciones corporativas, software de terceros y herramientas de desarrollo.	Clasificación de importancia, revisión de seguridad de aplicaciones.
Protocolos de Comunicación	Protocolos utilizados para la transmisión de datos.	Revisión de seguridad de protocolos, gestión de configuraciones.
Puntos de Acceso y Usuarios	Identificación de puntos de acceso a la red y usuarios autorizados.	Control de acceso, gestión de derechos de usuario.
Datos Sensibles	Ubicación de datos sensibles o críticos dentro de la red.	Clasificación y manejo de información según su categoría de seguridad.

Nota: Elaboración propia.

B) Identificación de requisitos de seguridad: se deben definir los requisitos específicos de seguridad de la red, basándose en el tipo de datos y los niveles de protección requeridos por la organización, como se los propone en la Tabla 7.

Tabla 7

Fase 1 Identificación de requisitos de seguridad

Requisito	Descripción	Criterios ISO/IEC 27001
Confidencialidad	Protección de información para asegurar el acceso solo a personas autorizadas.	Implementación de controles de acceso basados en la clasificación de la información.
Integridad	Garantizar que la información no sea alterada por no autorizados.	Uso de controles criptográficos y de integridad para proteger los datos.
Disponibilidad	Asegurar la disponibilidad de recursos de la red para los usuarios legítimos.	Estrategias de continuidad del negocio, respaldos y recuperación ante desastres.
Autenticación y Autorización	Verificación de la identidad de usuarios y asignación del nivel correcto de acceso.	Políticas de control de acceso, autenticación fuerte y gestión de identidades.
Gestión de Vulnerabilidades	Identificar, clasificar, remediar y mitigar vulnerabilidades de forma continua.	Evaluaciones de riesgos regulares, pruebas de penetración y análisis de vulnerabilidades.
Respuesta a Incidentes	Procedimientos para responder a brechas de seguridad.	Desarrollar e implementar una serie de acciones que permitan dar respuesta oportuna a incidentes relacionados con la seguridad informática.

Nota: Elaboración propia.

2. Selección de herramientas y tecnologías de IA

En la actualidad existen diferentes herramientas y soluciones que hacen uso de IA dentro de la seguridad informática. Por lo que, es necesario seleccionar una herramienta ajustada a los requerimientos y necesidad de la infraestructura y de datos de la red LAN. Para esto se deberán investigar soluciones de IA y hacer pruebas de las mismas.

A) Investigación de soluciones de IA: explorar y seleccionar herramientas de IA especializadas en análisis de seguridad y detección de vulnerabilidades, considerando aquellas que ofrezcan integración con la infraestructura existente. Entre las soluciones existentes se tienen las que muestra la Tabla 8.

Tabla 8

Fase 2 Soluciones de IA en el mercado

Solución	Características Principales	Costo	Nivel Destrezas del gestor de TI	Enlace Web
VirusTotal	Análisis gratuito y rápido de archivos y URLs para detectar malware, phishing y otras amenazas.	Gratis	Bajo	VirusTotal
Cyren	Plataforma de análisis de malware con IA que ofrece detección	Desde $49/mes	Medio	Cyren

	avanzada, sandboxing y análisis de comportamiento.			
Palo Alto Networks Cortex XDR	Solución de detección y respuesta extendida (XDR) que utiliza IA para identificar y responder a amenazas en tiempo real.	Desde $15,000/año	Alto	Cortex XDR
IBM Security QRadar	Plataforma de gestión de información y eventos de seguridad (SIEM) que utiliza IA para correlacionar eventos y detectar amenazas.	Desde $30,000/año	Alto	IBM QRadar
Microsoft Azure Sentinel	Solución de SIEM en la nube que utiliza IA para analizar datos de seguridad y detectar amenazas.	Desde $0.05/GB por hora	Medio	Azure Sentinel
Rapid7 InsightVM	Solución de gestión de vulnerabilidades que utiliza IA para identificar y priorizar vulnerabilidades en redes LAN.	Desde $14,995/año	Medio	InsightVM
QualysGuard VMDR	Solución de detección y respuesta a vulnerabilidades (VMDR) que utiliza IA para automatizar la respuesta a vulnerabilidades.	Desde $15,000/año	Alto	Qualys VMDR
Tenable Nessus	Solución de escaneo de vulnerabilidades que utiliza IA para identificar y priorizar vulnerabilidades en redes LAN.	Desde $2,995/año	Bajo	Tenable Nessus

Nota: Elaboración propia.

B) Pruebas de Herramientas: probar las herramientas en un entorno controlado para evaluar su efectividad en la detección de vulnerabilidades conocidas y en la generación de falsos positivos. A continuación, en la Tabla 9 un conjunto de pruebas recomendadas, junto con los criterios de evaluación y los resultados esperados.

Tabla 9

Fase 2 Pruebas de herramientas de IA

Prueba	Descripción	Criterios de Evaluación	Resultados Esperados
Detección de Vulnerabilidades	Evaluar la capacidad de la herramienta para identificar vulnerabilidades conocidas en la red LAN.	Precisión en la identificación, cobertura de tipos de vulnerabilidades.	Alta tasa de detección con baja incidencia de falsos negativos.

Identificación de Falsos Positivos	Probar la herramienta contra eventos benignos para evaluar la generación de falsos positivos.	Tasa de falsos positivos, capacidad de ajuste de la herramienta.	Mínima generación de falsos positivos.
Análisis de Comportamiento Anómalo	Verificar la habilidad de la herramienta para detectar comportamientos anómalos que podrían indicar una vulnerabilidad.	Sensibilidad en la detección de anomalías, capacidad de aprendizaje.	Detección efectiva de anomalías con un bajo número de alarmas irrelevantes.
Integración con la Infraestructura Existentes	Testear la compatibilidad y la facilidad de integración de la herramienta con la infraestructura de TI actual.	Facilidad de integración, compatibilidad con sistemas y protocolos existentes.	Integración sin problemas con la infraestructura de TI existente.
Respuesta a Incidentes	Evaluar la capacidad de la herramienta para generar alertas y facilitar la respuesta a incidentes.	Tiempo de respuesta, claridad y utilidad de las alertas.	Alertas oportunas y útiles que permiten una rápida respuesta a incidentes.
Facilidad de Uso y Soporte	Examinar la interfaz de usuario, documentación y soporte técnico proporcionados con la herramienta.	Intuitividad de la interfaz, calidad de la documentación, soporte técnico.	Herramienta fácil de usar con soporte técnico accesible y eficaz.

Nota: Elaboración propia.

3. Integración de datos y configuración

La integración de datos y configuración implica la consolidación y normalización de diversas fuentes de datos internas, como registros de red y sistemas de detección de intrusos, para su análisis mediante herramientas de inteligencia artificial (IA). Este proceso requiere las siguientes actividades:

A) Integración de fuentes de datos: implica asegurar la integración de las herramientas de IA con fuentes de datos internas (logs de red, sistemas de detección de intrusos) para el análisis, cuyas recomendaciones se muestran en la Tabla 10.

Tabla 10

Fase 3 Integración de datos y configuración

Acción	Descripción	Consideraciones Importantes
Identificación de Fuentes de Datos	Enumerar y evaluar todas las fuentes de datos internas disponibles, como logs de red, sistemas de detección de intrusos (IDS), y registros de aplicaciones.	Priorizar fuentes de datos basadas en relevancia y fiabilidad.
Acceso a Datos	Asegurar accesos apropiados a las fuentes de datos seleccionadas para la integración con las herramientas de IA.	Implementar políticas de seguridad para proteger el acceso a los datos.

Normalización de Datos	Estandarizar formatos de datos para asegurar compatibilidad con las herramientas de IA, incluyendo la conversión de formatos y la homogeneización de esquemas.	Utilizar prácticas estándar de ETL (Extract, Transform, Load).
Automatización de la Recolección	Automatizar el proceso de recolección de datos desde las fuentes identificadas para facilitar un flujo continuo de información hacia las herramientas de IA.	Implementar scripts o utilizar herramientas de automatización de procesos.
Validación de Datos	Realizar comprobaciones de calidad y veracidad de los datos para minimizar errores o información irrelevante que pueda afectar el análisis de IA.	Establecer rutinas periódicas de limpieza y validación de datos.
Integración Continua	Establecer procesos para la actualización y sincronización continua de datos entre las fuentes y las herramientas de IA.	Monitorizar y ajustar los flujos de datos para optimizar la integración.

Nota: Elaboración propia.

B) Configuración de parámetros de IA: en función de las herramientas seleccionadas se deberán configurar los parámetros necesarios para optimizar la detección de vulnerabilidades específicas de la red LAN. Para lo cual, se pueden seguir las siguientes recomendaciones que indica la Tabla 11

Tabla 11

Fase 3 Configuración de parámetros de IA

Acción	Descripción	Consideraciones Importantes
Selección de Modelos de IA	Elegir los modelos de IA más adecuados para el análisis de vulnerabilidades, basándose en las características de la red LAN.	Considerar modelos pre-entrenados o la necesidad de entrenamiento propio.
Ajuste de Parámetros	Configurar los parámetros de los modelos de IA, como el umbral de sensibilidad, para equilibrar la detección y los falsos positivos.	Realizar pruebas iterativas para encontrar el equilibrio óptimo.
Entrenamiento Personalizado	Si es posible, entrenar modelos de IA con datos específicos de la red LAN para mejorar la precisión en la detección de vulnerabilidades.	Utilizar un conjunto de datos representativo y actualizado.
Validación de Modelos	Analizar el funcionamiento de las herramientas configuradas, utilizando conjuntos de datos de prueba para asegurar su efectividad.	Ajustar modelos basándose en resultados de validación.
Integración de Alertas	Configurar la generación de alertas basadas en los resultados del análisis de IA, definiendo criterios para la notificación.	Integrar alertas con sistemas de gestión de incidentes existentes.
Actualización y Mantenimiento	Establecer un proceso para la revisión y actualización regular de los modelos de IA	Planificar revisiones periódicas para ajustar a la evolución del entorno de amenazas.

	y sus parámetros basados en nuevas amenazas.

Nota: Elaboración propia.

4. Desarrollo de capacidades de aprendizaje y adaptación

En esta fase implica entrenar y actualizar continuamente modelos de inteligencia artificial (IA) con datos de seguridad históricos y actuales, para mejorar su habilidad en identificar patrones de ataques y vulnerabilidades en redes LAN. Esto asegura que las herramientas de IA se mantengan efectivas ante los cambios en las amenazas, adaptándose a nuevas vulnerabilidades y técnicas de ataque. A continuación, en la Tabla 12 se muestran las acciones a seguir en este punto:

Tabla 12

Fase 4 Desarrollo de capacidades de aprendizaje y adaptación

Acción	Descripción	Consideraciones Importantes
Selección de datos para entrenamiento	Identificar y preparar conjuntos de datos históricos relevantes que incluyan registros de ataques, vulnerabilidades y anomalías.	Asegurar la diversidad y la representatividad de los datos.
Preprocesamiento de datos	Limpiar, normalizar y transformar los datos para el entrenamiento de IA, mejorando la eficacia del aprendizaje.	Manejar valores faltantes, eliminar duplicados, normalizar formatos.
Elección de modelos de IA	Seleccionar modelos de aprendizaje automático o aprendizaje profundo adecuados para la detección de vulnerabilidades.	Considerar modelos como redes neuronales, árboles de decisión, SVM, etc.
Entrenamiento y validación de modelos	Entrenar los modelos de IA con los datos preparados y validar su eficacia utilizando métricas de rendimiento.	Ajustar parámetros adicionales, realizar validación cruzada.
Implementación de aprendizaje continuo	Configurar los modelos para que se actualicen automáticamente con nuevos datos sobre vulnerabilidades y técnicas de ataque.	Utilizar técnicas como aprendizaje federado o transferencia de aprendizaje.
Pruebas de robustez y generalización	Evaluar la capacidad de los modelos para detectar nuevas y desconocidas vulnerabilidades, asegurando su adaptabilidad.	Realizar pruebas con datos recientes y escenarios simulados.
Retroalimentación y ajustes	Integrar mecanismos de retroalimentación para ajustar y mejorar los modelos de IA basados en los resultados y hallazgos.	Establecer un proceso iterativo de evaluación y ajuste de modelos.
Monitorización continua del rendimiento	Monitorear el desempeño de las herramientas de IA en tiempo real para detectar desviaciones y optimizar su funcionamiento.	Implementar dashboards y alertas para el seguimiento del rendimiento.

Actualización de conjuntos de datos	Asegurar una actualización regular de los conjuntos de datos utilizados para el entrenamiento con información reciente.	Incorporar datos sobre nuevas amenazas y vulnerabilidades detectadas.

Nota: Elaboración propia.

5. Automatización del proceso de detección

En la propuesta de análisis de vulnerabilidades en redes LAN, automatizar todas las actividades de detección con herramientas de IA, implica la implementación de escaneos de seguridad programados y la integración con sistemas de respuesta a incidentes. Esto permite identificar y responder a las vulnerabilidades de manera eficiente, minimizando el riesgo y optimizando los recursos de seguridad informática. A continuación, en la Tabla 13 se muestran una serie de acciones para esta etapa.

Tabla 13

Fase 5 Automatización de procesos de detección

Acción	Descripción	Consideraciones Importantes
Programación de escaneos de seguridad	Establecer una programación regular para los escaneos de seguridad que cubra toda la red LAN, utilizando las herramientas de IA seleccionadas.	Definir la frecuencia de los escaneos basada en el nivel de riesgo y las mejores prácticas de seguridad.
Personalización de escaneos	Configurar los escaneos de seguridad para enfocarse en áreas críticas de la red y ajustar la sensibilidad de detección según las necesidades específicas.	Ajustar configuraciones para equilibrar la exhaustividad del escaneo con el rendimiento de la red.
Integración con herramientas de IA	Asegurar que las herramientas de IA estén plenamente integradas con los sistemas de escaneo de seguridad, para una detección avanzada y análisis de vulnerabilidades.	Para todas las herramientas utilizadas es necesario hacer un análisis de la capacidad y compatibilidad de la información para que esta pueda ser procesada de forma adecuada.
Automatización de respuestas a incidentes	Vincular las herramientas de IA con sistemas de gestión de incidentes para que las respuestas a las vulnerabilidades detectadas se inicien automáticamente.	Configurar reglas de respuesta basadas en el tipo y la gravedad de la vulnerabilidad detectada.
Pruebas y ajustes	Realizar pruebas regulares del proceso automatizado para asegurar su correcto funcionamiento y realizar ajustes según sea necesario.	Incluir simulacros de incidentes para validar la efectividad de las respuestas automatizadas.
Actualización y mantenimiento	Mantener actualizadas las herramientas de IA y los sistemas de gestión de incidentes para asegurar una detección y respuesta óptimas ante nuevas vulnerabilidades.	Programar revisiones periódicas para actualizar software y ajustar configuraciones.

Documentación y capacitación	Documentar el proceso de automatización y ofrecer capacitación relevante al equipo de TI y seguridad para su operación y mantenimiento.	Asegurar que el equipo comprenda el flujo de trabajo automatizado y cómo intervenir cuando sea necesario.

Nota: Elaboración propia.

6. Monitoreo y análisis continúo

El monitoreo y análisis continuo se refiere a la vigilancia constante de la red para detectar cualquier actividad sospechosa o potencial vulnerabilidad de forma inmediata. Esto incluye la evaluación precisa de las alertas generadas por las herramientas de IA, distinguiendo entre amenazas reales y falsos positivos, y ajustando la configuración de las herramientas para mejorar su precisión y eficacia. La Tabla 14 muestran las acciones a seguir en esta etapa.

Tabla 14

Fase 6 Monitoreo y análisis continuo

Acción	Descripción	Consideraciones Importantes
Configuración de monitoreo	Establecer sistemas de monitoreo en tiempo real que cubran toda la red LAN, utilizando las herramientas de IA para la detección de anomalías y vulnerabilidades.	Asegurar cobertura completa y minimizar áreas ciegas en la red.
Evaluación de alertas	Revisar y clasificar las alertas generadas por las herramientas de IA para identificar amenazas legítimas y falsos positivas.	Priorizar alertas basadas en severidad y potencial impacto.
Ajuste de herramientas de IA	Modificar la configuración de las herramientas de IA según el análisis de las alertas para afinar la detección y reducir los falsos positivos.	Realizar ajustes basados en tendencias observadas y retroalimentación.
Integración de fuentes de datos	Incorporar continuamente nuevas fuentes de datos a las herramientas de IA para enriquecer el análisis y mejorar la detección de vulnerabilidades.	Explorar fuentes de datos externas e internas para una visión completa.
Análisis de tendencias	Utilizar las herramientas de IA para analizar tendencias y patrones en las alertas y las vulnerabilidades detectadas.	Identificar posibles campañas de ataque o vulnerabilidades emergentes.

Reportes y documentación	Generar reportes detallados sobre las alertas, las acciones tomadas y los ajustes realizados, manteniendo una documentación completa para auditorías futuras.	Utilizar los reportes para revisión estratégica y mejora continua.

Nota. Elaboración propia

7. **Capacitación y sensibilización**

La capacitación y sensibilización se refiere al proceso de educar tanto al equipo de TI como a los usuarios finales sobre la importancia de las prácticas seguras de navegación y la gestión eficiente de las herramientas de IA. Esta formación busca no solo mejorar las habilidades técnicas del personal de TI en la detección y respuesta a vulnerabilidades sino también elevar la conciencia en los usuarios sobre la seguridad de datos, reduciendo así el riesgo de incidentes. A continuación, en la Tabla 15 se proponen las acciones recomendadas:

Tabla 15

Fase 7 Capacitación y sensibilización

Acción	Descripción	Consideraciones Importantes
Desarrollo del programa de formación	Crear un currículo detallado para la capacitación del equipo de TI, enfocándose en herramientas de IA, prácticas de seguridad en la red LAN, y procedimientos de respuesta ante incidentes.	Asegurar que el contenido sea relevante y actualizado.
Sesiones de capacitación de TI	Organizar sesiones de formación regulares para el personal de TI, incluyendo talleres prácticos y simulaciones de escenarios de vulnerabilidades.	Fomentar la participación activa y el aprendizaje práctico.
Materiales de aprendizaje	Desarrollar y distribuir materiales de aprendizaje, como guías, tutoriales en vídeo y FAQs sobre seguridad y uso de las herramientas de IA.	Facilitar el acceso a recursos de aprendizaje continuo.
Programas de concienciación para usuarios	Implementar sesiones de sensibilización sobre seguridad en la red para usuarios finales, destacando la importancia de contraseñas fuertes, y otras prácticas seguras.	Personalizar el contenido para diferentes audiencias de usuarios.
Evaluaciones y retroalimentación	Realizar evaluaciones periódicas para medir la efectividad de las capacitaciones ajustando los métodos y materiales según sea necesario.	Utilizar la retroalimentación para mejorar continuamente los programas.
Actualización continua	Mantener los programas de capacitación y materiales de aprendizaje actualizados con las últimas tendencias de seguridad y tecnologías de IA.	Adaptarse a la evolución del panorama de amenazas.
Promoción de una cultura de seguridad	Incentivar una cultura de seguridad dentro de la organización, reconociendo las buenas prácticas y fomentando la comunicación abierta sobre los riesgos de seguridad.	Reconocer y recompensar las contribuciones positivas a la seguridad.

8. Revisión y mejora continúa

La revisión y mejora continua implica un proceso sistemático y periódico de evaluación de la efectividad de las herramientas y estrategias implementadas. Este proceso está diseñado para identificar áreas de mejora, asegurar que las herramientas de IA estén alineadas con las últimas tendencias en ciberseguridad, y adaptar las prácticas de seguridad a las cambiantes condiciones y amenazas del entorno. Dentro de esta etapa se han planteado diferentes acciones dentro del contexto de la revisión y mejora continua, como indica la Tabla 16.

Tabla 16

Fase 8 Revisión y mejora continua

Acción	Descripción	Consideraciones Importantes
Programación de revisiones periódicas	Establecer un calendario para las revisiones regulares de las herramientas y prácticas de IA en la detección de vulnerabilidades.	Asegurar consistencia en la evaluación de la eficacia de las herramientas.
Evaluación de desempeño	Medir el desempeño de las herramientas de IA mediante el análisis de métricas específicas, como la precisión en la detección y la tasa de falsos positivos.	Utilizar datos históricos y comparativos para evaluar el progreso.
Análisis de incidentes de seguridad	Revisar y analizar los incidentes de seguridad recientes para identificar posibles fallos o deficiencias en la detección de vulnerabilidades.	Aprender de los incidentes para mejorar las estrategias de detección.
Actualización de herramientas de IA	Mantener las herramientas de IA actualizadas con las últimas versiones y tecnologías disponibles para mejorar la eficacia en la detección.	Seguir de cerca los avances en IA y ciberseguridad para implementar mejoras.
Capacitación continua del equipo	Proporcionar formación actualizada al equipo de TI sobre las últimas herramientas, técnicas y tendencias en IA y ciberseguridad.	Fomentar el desarrollo profesional continuo y la adaptabilidad del equipo.
Retroalimentación y sugerencias	Recopilar retroalimentación del equipo de TI y usuarios finales sobre la efectividad de las herramientas y estrategias de seguridad implementadas.	Utilizar esta información para realizar ajustes informados y dirigidos.
Ajustes basados en tendencias	Ajustar las herramientas y estrategias de detección de vulnerabilidades basándose en las tendencias emergentes y el cambiante panorama de amenazas.	Mantener la seguridad de la red proactiva y relevante frente a nuevas vulnerabilidades.

Nota: Elaboración propia.

2.3 Validación de la propuesta

La propuesta de recomendaciones para el análisis de vulnerabilidades basado en IA para redes LAN, fue validada por parte de expertos en el campo de la seguridad informática.

Los especialistas que aportaron esta evaluación fueron: Msc. Jorge Jairo Yaguar Mariño y la Msc. Paola Carolina Mejía Quinteros.

Para asegurar una valoración objetiva se empleó una escala de Likert según los siguientes criterios (ver anexo 1):

Impacto: la propuesta ha sido calificada como altamente impactante, considerando su potencial para fortalecer las medidas de seguridad en redes de área local mediante la aplicación de tecnologías de inteligencia artificial.

Aplicabilidad: se reconoce la aplicabilidad directa de las técnicas propuestas en entornos corporativos reales, resaltando la viabilidad de su implementación en diversas estructuras organizativa.

Conceptualización: la propuesta ha sido valorada positivamente en términos de su solidez conceptual, mostrando un entendimiento de la aplicación de la inteligencia artificial en el ámbito de la seguridad informática.

Actualidad: los evaluadores confirmaron que la investigación se sitúa en la vanguardia del conocimiento, abordando tecnologías emergentes y respondiendo a las necesidades actuales de seguridad informática

Calidad técnica: la calidad técnica de la propuesta ha sido destacada, evidenciando atributos cualitativos claros para los beneficiarios.

Factibilidad: la evaluación señala que la implementación de las técnicas de inteligencia artificial propuestas es factible, considerando tanto los recursos tecnológicos disponibles actualmente como la capacidad de adaptación de las organizaciones a estas nuevas herramientas.

Pertinencia: finalmente, la propuesta aborda de manera directa y efectiva los retos actuales en la protección de infraestructuras críticas de información y la prevención de ciberataques en redes de área local.

2.4 Matriz de articulación de la propuesta

En la Tabla 17 se presenta matriz de articulación que sintetiza el producto realizado con los sustentos teóricos y metodológicos.

Tabla 17

Matriz de articulación

Ejes o partes principales	Sustento teórico	Sustento metodológico	Estrategias / técnicas	Descripción de resultados	Instrumentos aplicados
Seguridad informática	La seguridad informática comprende una serie de estrategias y prácticas destinadas a proteger los sistemas informáticos, asegurando que se utilicen adecuadamente y sin interferencias externas no autorizadas (Miranda Vera, 2019).	La metodología de investigación fue documental que permitió tener los conceptos y criterios actualizados sobre seguridad informática	Fuentes bibliográficas	Definir los principales conceptos relacionados con la seguridad informática y vulnerabilidades en redes LAN	Resumen Tablas
Inteligencia artificial	La Inteligencia Artificial (IA) se ha reconocido como la facultad de las máquinas para adaptarse, solucionar problemas y ejecutar tareas que implican inteligencia. (Martínez-Comesaña et al., 2023).	La metodología de investigación fue documental que permitió tener los conceptos y criterios actualizados sobre inteligencia artificial	Fuentes bibliográficas	Se recopilan los principales usos que puede presentar la IA dentro aplicaciones de seguridad informativa, como lo es la detección de vulnerabilidades en redes LAN.	Resumen Tablas
Fase 1 Evaluación inicial y definición de requisitos	Mediante esta fase se realiza un inventario de la infraestructura de red LAN actual, identificando dispositivos, sistemas, y aplicaciones críticas.	Revisión documental	Fuentes bibliográficas	Auditorias de infraestructura Identificación de requisitos de seguridad.	Controles, evaluación del riesgo.

Fase 2 Selección de herramientas y tecnologías de IA	En la actualidad existen diferentes herramientas y soluciones que hacen uso de IA dentro de la seguridad informática. Por lo que, es necesario seleccionar una herramienta ajustada a los requerimientos y necesidad de la infraestructura y de datos de la red LAN	Revisión documental	Fuentes bibliográficas	Soluciones de IA en el mercado Pruebas de funcionamiento	Pruebas de detección de falsos positivos y falsos negativos. Detección de alertas oportunas
Fase 3 Integración de datos y configuración	La integración de datos y configuración implica la consolidación y normalización de diversas fuentes de datos internas, como registros de red y sistemas de detección de intrusos, para su análisis mediante herramientas de inteligencia artificial (IA).	Revisión documental	Fuentes bibliográficas	Identificación y acceso a datos. Normalización de datos Automatización y recolección Configuración de parámetros de IA	Practicas estándar ETL Rutinas de limpieza y validación de datos. Modelos de validación
Fase 4 Desarrollo de capacidades de aprendizaje y adaptación	En esta fase implica entrenar y actualizar continuamente modelos de inteligencia artificial (IA) con datos de seguridad históricos y actuales, para mejorar su habilidad en identificar patrones de ataques y vulnerabilidades en redes LAN	Revisión documental	Fuentes bibliográficas	Datos de entrenamiento Validación de modelo Monitoreo y ajustes Datos de nuevas amenazas	Pruebas y simulaciones Dashboards de alertas y seguimiento Pruebas de robustez
Fase 5 Automatización del proceso de detección	Automatizar todas las actividades de detección con herramientas de IA, implica la implementación de escaneos de seguridad programados y la integración con sistemas de respuesta a incidentes.	Revisión documental	Fuentes bibliográficas	Programación de escaneos y seguridad Integración de herramientas de IA Actualización y mantenimiento	Documentos y registros

Fase 6 Monitoreo y análisis continuo	El monitoreo y análisis continuo se refiere a la vigilancia constante de la red para detectar cualquier actividad sospechosa o potencial vulnerabilidad de forma inmediata	Revisión documental	Fuentes bibliográficas	Evaluación de alertas Ajuste de herramientas de IA Análisis tendencias	Documentos y registros
Fase 7 Capacitación y sensibilización	La capacitación y sensibilización se refiere al proceso de educar tanto al equipo de TI como a los usuarios finales sobre la importancia de las prácticas seguras de navegación y la gestión eficiente de las herramientas de IA.	Revisión documental	Fuentes bibliográficas	Programas de concienciación de los usuarios Promoción de cultura de seguridad	Documentos y registros
Fase 8 Revisión y mejora continua	Este proceso está diseñado para identificar áreas de mejora, asegurar que las herramientas de IA estén alineadas con las últimas tendencias en ciberseguridad, y adaptar las prácticas de seguridad a las cambiantes condiciones y amenazas del entorno	Revisión documental	Fuentes bibliográficas	Análisis de incidentes de seguridad Retroalimentación y sugerencias. Actualización de sistemas de IA	Documentos y registros

Nota: Elaboración propia.

CONCLUSIONES

La investigación ha mostrado que hacer uso de técnicas y herramientas de de inteligencia artificial en el análisis de vulnerabilidades en redes LAN ayuda a mejorar la capacidad de detección y respuesta los riesgos de posibles amenazas cibernéticas. Una IA bien entrenada permite identificar de forma rápida y precisa de patrones de ataque complejos, mejorando la seguridad informática sin incrementar proporcionalmente los recursos humanos o técnicos necesarios para su gestión.

Los hallazgos subrayan que el éxito de la integración de la IA en la seguridad de redes LAN no solo depende de la tecnología en sí, sino también de la capacitación del equipo de TI y la sensibilización de los usuarios finales. Una formación adecuada permite maximizar las capacidades y características de las herramientas de IA, mientras que fomentar una cultura de seguridad informática reduce significativamente la probabilidad de incidentes.

La automatización de escaneos de seguridad y la implementación de aprendizaje continuo en las herramientas de IA destacan como prácticas efectivas para mantener una defensa proactiva y resiliente. Estas estrategias garantizan no solo una vigilancia constante de la red LAN, sino también la adaptabilidad de las herramientas frente a nuevas y evolutivas amenazas.

Los resultados obtenidos enfatizan la relevancia de realizar evaluaciones periódicas de las herramientas de IA y su eficacia en el contexto específico de la seguridad LAN. Esta práctica permite identificar oportunamente áreas de mejora y ajustar la configuración de las herramientas para optimizar los parámetros para la detección de vulnerabilidades, destacando la capacidad de respuesta rápida como un diferenciador crítico en la protección efectiva de la red.

RECOMENDACIONES

Se recomienda que los equipos de TI en las organizaciones procedan a la adopción e integración de tecnologías de inteligencia artificial específicamente diseñadas para la detección de vulnerabilidades en redes LAN. Esta acción debe ser llevada a cabo por especialistas en seguridad informática, quienes, mediante la configuración adecuada y la optimización continua de estas herramientas, pueden lograr una identificación más eficaz y eficiente de amenazas, resultando en una mejora en la capacidad de respuesta sin requerir un aumento proporcional en los recursos asignados a la seguridad informática.

Es necesario desarrollar y ejecutar programas de formación y sensibilización dirigidos tanto al personal de TI como a los usuarios finales, enfocando en las buenas prácticas de seguridad y el uso efectivo de las herramientas de IA. Esta recomendación implica que los responsables de seguridad informática y recursos humanos colaboren estrechamente para diseñar e implementar estas iniciativas. El resultado esperado es una mayor conciencia sobre la seguridad en toda la organización y una reducción en la incidencia de vulnerabilidades explotables por falta de conocimiento o negligencia.

Se aconseja establecer y mantener procesos automatizados para los escaneos de seguridad, junto con mecanismos de aprendizaje continuo para las herramientas de IA. Los administradores de sistemas y equipos de seguridad deberían ser los encargados de implementar estas prácticas, asegurando así una monitorización ininterrumpida y una adaptación ágil a nuevas amenazas. Como resultado, se anticipa una defensa más robusta y proactiva de la red LAN, capaz de responder a un espectro más amplio de vulnerabilidades y ataques.

Finalmente, es aconsejable llevar a cabo revisiones periódicas sobre la eficacia de las soluciones de IA para la identificación de fallos de seguridad en las redes de área local. Esta responsabilidad recae en el equipo de seguridad de TI, cuya meta es descubrir y aplicar las modificaciones pertinentes en la configuración de dichas herramientas para optimizar su funcionamiento. Como resultado, se espera lograr un avance constante en las capacidades de detección y reacción ante incidentes, asegurando así que la infraestructura de red permanezca resguardada de forma efectiva y se mantenga al día frente a las nuevas tendencias y retos en el campo de la ciberseguridad.

BIBLIOGRAFÍA

3digits, S. de I. I. (2019). *3digits – Tenemos una solución – Tecnologías de la Información* (Palma, Mallorca, España). https://www.3digits.es/blog/ia-en-seguridad-informatica.html

Alom, M. Z., Taha, T. M., Yakopcic, C., Westberg, S., Sidike, P., Nasrin, M. S., Van Esesn, B. C., Awwal, A. A. S., & Asari, V. K. (2018). *The History Began from AlexNet: A Comprehensive Survey on Deep Learning Approaches* (arXiv:1803.01164). arXiv. https://doi.org/10.48550/arXiv.1803.01164

AMBIT-BST. (2023). *Diferencias entre amenaza, vulnerabilidad y riesgo*. https://www.ambit-bst.com/blog/diferencias-entre-amenaza-vulnerabilidad-y-riesgo

Azan Basallo, Y., Senti, V., & Sanchez, N. (2018). Artificial intelligence techniques for information security risk assessment. *IEEE Latin America Transactions*, *16*, 897-901. https://doi.org/10.1109/TLA.2018.8358671

Bardají, E. (2022). *La inteligencia artificial como aliada para prevenir ciberataques*. https://www.esedsl.com/blog/la-inteligencia-artificial-como-aliada-para-prevenir-ciberataques

Carballar, J. A. (2021, octubre 8). Seguridad de una red de área local o LAN. *Carballar.com*. https://carballar.com/seguridad-de-una-red-de-area-local-o-lan

Dempsey, J. (2021). *Managing the Cybersecurity Vulnerabilities of Artificial Intelligence*. Default. https://www.lawfaremedia.org/article/managing-cybersecurity-vulnerabilities-artificial-intelligence

Eian, I. C., Yong, L. K., Li, M. Y. X., Qi, Y. H., & Z, F. (2020). *Cyber Attacks in the Era of COVID-19 and Possible Solution Domains* (2020090630). Preprints. https://doi.org/10.20944/preprints202009.0630.v1

Hernández Yeja, A. (2013). Aplicación de técnicas de inteligencia artificial en la seguridad informática: Un estudio. *Inteligencia artificial revista iberoamericana de inteligencia artificial*.

IBM. (2021, abril 14). *Estándares de red de área local*. https://www.ibm.com/docs/es/i/7.2?topic=standards-local-area-network

IBM. (2022). *What is an AI model?* https://www.ibm.com/topics/ai-model

Kommrush, S. (2018). Artificial Intelligence Techniques for Security Vulnerability Prevention. *Cornell University*. https://doi.org/10.48550/arXiv.1912.06796

Martínez-Comesaña, M., Rigueira-Díaz, X., Larrañaga-Janeiro, A., Martínez-Torres, J., Ocarranza-Prado, I., & Kreibel, D. (2023). Impacto de la inteligencia artificial en los métodos de evaluación en la educación primaria y secundaria: Revisión sistemática de la literatura. *Revista de Psicodidáctica*, *28*(2), 93-103. https://doi.org/10.1016/j.psicod.2023.06.001

Miranda, C. K. (2019). *Estudio de Riesgos y Vulnerabilidades de la Red LAN y Equipos del Infocentro San Juan* [bachelorThesis, Babahoyo, UTB 2019]. http://dspace.utb.edu.ec/handle/49000/6901

NSFOCUS. (2023, octubre 12). *Countdown to GovWare 2023—The Application of Artificial Intelligence (AI) in Cybersecurity*. NSFOCUS, Inc., a global network and cyber security leader, protects enterprises and carriers from advanced cyber attacks. https://nsfocusglobal.com/countdown-to-govware-2023-the-application-of-artificial-intelligence-ai-in-cybersecurity/

NVD. (2023). Estadísticas y hechos de vulnerabilidad de seguridad cibernética en 2022. *Ciberseguridad*. https://ciberseguridad.com/amenzas/vulnerabilidades/estadisticas/

OHCHR. (2021). *Los riesgos de la inteligencia artificial para la privacidad exigen medidas urgentes –Bachelet*. OHCHR. https://www.ohchr.org/es/press-releases/2021/09/artificial-intelligence-risks-privacy-demand-urgent-action-bachelet

Ovallos, J., Rico-Bautista, D., & Medina-Cárdenas, Y. (2020). A practical guide to analyzing vulnerabilities in a GNU/Linux client-server environment using a pentesting methodology. *RISTI - Revista Iberica de Sistemas e Tecnologias de Informacao*, *2020*, 335-350.

Qiu, J. (2016). *A survey of machine learning for big data processing | EURASIP Journal on Advances in Signal Processing*. https://link.springer.com/article/10.1186/s13634-016-0355-x

Ramasubramanian, K., Venkateswarlu, L., & Yerram, S. (2021). Applications and Techniques of Artificial Intelligence in Cyber Security. *Turkish Journal of Computer and Mathematics Education*, *12*(14), 332-339.

Rasthofer, S., & Arzt, S. (2014). A Machine-learning Approach for Classifying and Categorizing Android Sources and Sinks. *Internet Society*. http://www.bodden.de/pubs/rab14classifying.pdf.

Scaler. (2024, enero 7). *Top 10 Characteristics of Artificial Intelligence*. InterviewBit. https://www.interviewbit.com/blog/characteristics-of-artificial-intelligence/

Suárez Panchana, L. C. (2022). *Análisis de vulnerabilidad en la red Lan usando herramientas de hacking ético para una empresa de la provincia de Santa Elena* [bachelorThesis, La Libertad: Universidad Estatal Península de Santa Elena. 2022]. https://repositorio.upse.edu.ec/handle/46000/7727

Teigens, V., Skalfist, P., & Mikelsten, D. (s. f.). *Inteligencia artificial: La cuarta revolución industrial*. Cambridge Stanford Books.

Torres, A., & Rendón, F. (2020). *Revisión de las técnicas de inteligencia artificial aplicadas en seguridad informática*. *8*, 97-115. https://doi.org/10.21158/23823399.v7.n0.2019.2612

Wazid, M., Das, A. K., Chamola, V., & Park, Y. (2022). Uniting cyber security and machine learning: Advantages, challenges and future research. *ICT Express*, *8*(3), 313-321. https://doi.org/10.1016/j.icte.2022.04.007

Zeadally, S., Adi, E., Baig, Z., & Khan, I. A. (2020). Harnessing Artificial Intelligence Capabilities to Improve Cybersecurity. *IEEE Access*, *8*, 23817-23837. https://doi.org/10.1109/ACCESS.2020.2968045

Zhang, Z., Ning, H., Shi, F., Farha, F., Xu, Y., Xu, J., Zhang, F., & Choo, K.-K. R. (2022). Artificial intelligence in cyber security: Research advances, challenges, and opportunities. *Artificial Intelligence Review*, *55*(2), 1029-1053. https://doi.org/10.1007/s10462-021-09976-0

ANEXOS Anexo 1.

Encuesta

Análisis de vulnerabilidades de redes LAN con Inteligencia Artificial

Estimado/a administrador/a de TI y seguridad informática,

Le invitamos cordialmente a participar en la siguiente encuesta que tiene como objeitvo evaluar las necesidades actuales de los profesionales de TI y seguridad informática, para desarrollar soluciones de análisis de vulnerabilidades mediante la aplicación de técnicas de inteligencia artificial en redes de área local LAN.

1. ¿Cuenta su organización con una solución de análisis de vulnerabilidades para la seguridad informática actualmente?

- ○ SI
- ○ No

2. ¿Considera que la integración de la inteligencia artificial podría mejorar la detección de vulnerabilidades en su red de área local?

- ○ Si
- ○ No
- ○ No estoy segura/o

3. ¿Qué frecuencia de monitoreo de seguridad considera adecuada para su organización?

- ○ 24/7
- ○ Diaria
- ○ Semanal
- ○ Mensual

4. ¿Ha enfrentado su organización alguna violación de seguridad en los últimos 12 meses?

- ○ Si
- ○ No

5. En términos de seguridad informática, ¿cuál es el mayor desafío que enfrenta su organización?

- ○ Identificación de nuevas vulnerabilidades
- ○ Falta de herramientas automatizadas
- ○ Limitaciones en el personal de TI
- ○ Presupuesto restringido

6. ¿Su organización proporciona formación regular sobre seguridad informática a los empleados?

- Si
- No

7. ¿Qué nivel de personalización espera de una herramienta de IA para análisis de vulnerabilidades?

- Muy alto
- Mediano
- Poco
- No es importante

8. ¿Qué tan satisfecho está con las herramientas de seguridad informática actuales en cuanto a su capacidad de integración con otros sistemas?

- Muy satisfecho
- Satisfecho
- Insatisfecho
- Muy insatisfecho

9. ¿La alta dirección de su empresa está comprometida con las inversiones en seguridad informática?

- Si
- No
- No estoy segura/o

10. ¿Su organización realiza revisiones y mejoras continuas de las políticas de seguridad informática?

- Si
- No

Anexo 2. Instrumentos de validación de la propuesta

INSTRUMENTO DE VALIDACIÓN

UNIVERSIDAD TECNOLÓGICA ISRAEL

ESCUELA DE POSGRADOS "ESPOG"

MAESTRÍA EN SEGURIDAD INFORMÁTICA

INSTRUMENTO PARA VALIDACIÓN DE LA PROPUESTA

Estimado colega:

Se solicita su valiosa cooperación para evaluar la siguiente propuesta del proyecto de titulación: Análisis de Vulnerabilidades basado en Técnicas de Inteligencia Artificial para la Seguridad Informática en Redes de Área Local.

Sus criterios son de suma importancia para la realización de este trabajo, por lo que se le pide brinde su cooperación contestando las preguntas que se realizarán a continuación.

Datos informativos

Validado por: Ing. Mejía Quinteros Paola Carolina. MsC.

Titulo obtenido
MAGISTER EN TECNOLOGIAS DE LA INFORMACION MENCIÓN EN GESTION Y ADMINISTRACION DE TECNOLOGIA
Cédula de Identidad
1600376790
E- mail
carolmejia1708@hotmail.com
Institución de Trabajo
EMAPAST EP
Cargo
JEFE DEL AREA DE TICS
Años de experiencia en el área
14 años

Instructivo:

Responda cada criterio con la máxima sincera del caso;
Revisar, observar y analizar la propuesta del proyecto de titulación; y,
Coloque **una X** en cada indicador, tomando en cuenta que Muy adecuado equivale a 5, Bastante Adecuado equivale a 4, Adecuado equivale a 3, Poco Adecuado equivale a 2 e Inadecuado equivale a 1.

Tema:

Indicador	*Descripción*	Muy adecuado	Bastante Adecuado	Adecuado	Poco adecuado	Inadecuado
Impacto	*El alcance que tendrá la propuesta y su representatividad en la generación de valor*	5				
Aplicabilidad	*La capacidad de implementación de la propuesta considerando que los contenidos sean aplicables*	5				
Conceptualización	*La base de conceptos y teorías propias de la propuesta de manera sistémica y articulada*	5				
Actualidad	*Los procedimientos actuales y los cambios científicos y tecnológicos considerados en la propuesta*	5				
Calidad Técnica	*Los atributos cualitativos del contenido de la propuesta para satisfacer las expectativas de sus beneficiarios*	5				
Factibilidad	*El nivel de utilización de la propuesta por parte de la organización acorde a los recursos disponibles*	5				
Pertinencia	*La contundencia y conveniencia de la propuesta para solucionar el problema planteado*		4			
Total		34				

Observaciones:

El proyecto de investigación contribuye a la mitigación de ataques y amenazas a través del, Análisis de Vulnerabilidades basado en Técnicas de Inteligencia Artificial para la Seguridad Informática en Redes de Área Local.

Recomendaciones

Esta clase de trabajos investigativos, aportan al desarrollo y protección de datos e información que en la actualidad se han visto vulnerados, por lo que se recomienda que la institución siga promoviendo la investigación y desarrollo de estos temas que trascienden en la actualidad y contribuyen a la sociedad.

Lugar, fecha de validación: Puyo, 9 de marzo del 2024

Firma del especialista

2

INSTRUMENTO DE VALIDACIÓN

UNIVERSIDAD TECNOLÓGICA ISRAEL

ESCUELA DE POSGRADOS "ESPOG"

MAESTRÍA EN SEGURIDAD INFORMÁTICA

INSTRUMENTO PARA VALIDACIÓN DE LA PROPUESTA

Estimado colega:

Se solicita su valiosa cooperación para evaluar la siguiente propuesta del proyecto de titulación: Análisis de Vulnerabilidades basado en Técnicas de Inteligencia Artificial para la Seguridad Informática en Redes de Área Local.

Sus criterios son de suma importancia para la realización de este trabajo, por lo que se le pide brinde su cooperación contestando las preguntas que se realizan a continuación.

Datos informativos

Validado por: Ing. Yaguar Mariño Jorge Jairo MsC.

Título obtenido
MAGISTER EN INFORMATICA EMPRESARIAL
Cédula de Identidad
1600295628
E- mail
jyaguar@hotmail.com
Institución de Trabajo
GOBIERNO AUTÒNOMO DESCENTRALIZADO PROVINCIAL DE PASTAZA
Cargo
JEFE TECNOLOGIAS DE LA INFORMACION Y COMUNICACION
Años de experiencia en el área
17 años

Instructivo:

Responda cada criterio con la máxima sincera del caso;
Revisar, observar y analizar la propuesta del proyecto de titulación; y,
Coloque **una X** en cada indicador, tomando en cuenta que Muy adecuado equivale a 5, Bastante Adecuado equivale a 4, Adecuado equivale a 3, Poco Adecuado equivale a 2 e Inadecuado equivale a 1.

Tema: Análisis de Vulnerabilidades basado en Técnicas de Inteligencia Artificial para la Seguridad Informática en Redes de Área Local.

Indicador	*Descripción*	Muy adecuado	Bastante Adecuado	Adecuado	Poco adecuado	Inadecuado
Impacto	*El alcance que tendrá la propuesta y su representatividad en la generación de valor*	5				
Aplicabilidad	*La capacidad de implementación de la propuesta considerando que los contenidos sean aplicables*	5				
Conceptualización	*La base de conceptos y teorías propias de la propuesta de manera sistémica y articulada*	5				
Actualidad	*Los procedimientos actuales y los cambios científicos y tecnológicos considerados en la propuesta*	5				
Calidad Técnica	*Los atributos cualitativos del contenido de la propuesta para satisfacer las expectativas de sus beneficiarios*	5				
Factibilidad	*El nivel de utilización de la propuesta por parte de la organización acorde a los recursos disponibles*	5				
Pertinencia	*La contundencia y conveniencia de la propuesta para solucionar el problema planteado.*	5				
Total		35				

Observaciones:

El tema desarrollado en la investigación, genera un aporte sustancial al manejo de la seguridad informática. Aportará al desarrollo de actividades que permitan garantizar la confidencialidad, integridad y disponibilidad en el manejo de la información concerniente a la seguridad informática que cada día presenta nuevos desafíos.

Recomendaciones

Como alcance al presente proyecto de análisis, se debe seguir desarrollando nuevos estudios para complementar y enriquecer los conocimientos en par al desarrollo actual y los escenarios que comprenden al manejo de la IA y la ciberseguridad.

Lugar, fecha de validación: Puyo, 9 de marzo del 2024

Firma del especialista

Anexo. Matriz para valorar el impacto de la interacción de la IA con respecto a la seguridad informática

Fase de la Propuesta	Dimensión Evaluada	Características que la aporta la IA	Impacto Esperado en Seguridad Informática (Redes LAN)
Evaluación inicial y definición de requisitos	Eficiencia en la identificación de necesidades	• Capacidad de la IA para detectar requisitos específicos de la red LAN. • Velocidad de evaluación comparada con métodos tradicionales.	Impacto Alto Mejora en la precisión de los requisitos de seguridad basados en el contexto específico de la red.
Selección de herramienta de IA	Adecuación de la herramienta	• Conformidad de la herramienta de IA con las necesidades identificadas. • Capacidad de integración con sistemas existentes.	Impacto Alto Selección de una herramienta de IA más alineada con las necesidades de la red, potenciando la protección de la misma.
Integración de datos y configuración	Calidad de la integración	• Nivel de automatización en la recopilación y fusión de datos. • Complejidad de la configuración inicial.	Impacto Alto Reducción del tiempo de integración y aumento de la robustez en la detección de amenazas.
Monitoreo continuo	Detección de amenazas y respuesta	• Tasa de detección de amenazas reales vs falsos positivos. • Tiempo de respuesta ante incidentes.	Impacto Alto Mejora en la capacidad de vigilancia y respuesta rápida, manteniendo la integridad de la red LAN.
Desarrollo de entrenamiento y aprendizaje	Evolución del aprendizaje de la IA	• Mejora en la precisión de la IA con el tiempo. • Capacidad de adaptarse a nuevas amenazas.	Impacto Alto Aumento de la eficacia de la IA en la identificación de vulnerabilidades y amenazas emergentes.
Automatización de procesos de detección	Autonomía operativa	• Reducción de la intervención humana en la detección de amenazas. • Mejoras en la gestión del tiempo de los analistas de seguridad.	Impacto Alto Mayor eficiencia operativa, permitiendo que el personal se enfoque en tareas de mayor valor añadido.
Formación	Capacitación del personal	• Facilidad de uso de las herramientas de IA. • Cantidad de formación requerida para el personal de seguridad.	Impacto medio Personal mejor preparado para interactuar con las herramientas de IA, mejorando la postura de seguridad.
Revisión y mejora continua	Adaptabilidad y actualización	• Frecuencia y eficacia de las actualizaciones. • Capacidad de la IA para incorporar retroalimentación	Impacto Alto Un ciclo de mejora continua que se adapta a las cambiantes necesidades de seguridad de la red LAN.